现代数学基础丛书 169

有限p群构造

（下 册）

张勤海　安立坚　著

科学出版社

(O-6861.31)

www.sciencep.com



科学出版社互联网入口
科学数理分社
电 话：(010) 64019814
Email:lijingke@mail.sciencep.com
销售分类建议：高等数学



定 价：139.00 元

现代数学基础丛书 169

有限 p 群构造

（下 册）

张勤海 安立坚 著



科 学 出 版 社

北 京

内 容 简 介

全书分上下册出版. 下册介绍我国学者在交换性较强和正规性较强的 p 群的结构、临界 p 群及 p 群其他方面的成果.

本书供高等院校数学专业群论研究生及有关研究人员阅读, 也可供数学史研究人员参考.

图书在版编目（CIP）数据

有限 p 群构造. 下册/张勤海, 安立坚著. —北京：科学出版社, 2017.5
(现代数学基础丛书; 169)
ISBN 978-7-03-052831-5

Ⅰ. ①有… Ⅱ. ①张… ②安… Ⅲ. ①有限群 Ⅳ. ①O152.1

中国版本图书馆 CIP 数据核字 (2017) 第 107947 号

责任编辑: 李静科／责任校对: 张凤琴
责任印制: 张 伟／封面设计: 陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码: 100717
http://www.sciencep.com

北京教图印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2017 年 5 月第 一 版 开本: 720×1000 1/16
2017 年 5 月第一次印刷 印张: 23 3/4
字数: 460 000

定价: 139.00 元

(如有印装质量问题, 我社负责调换)

《现代数学基础丛书》序

对于数学研究与培养青年数学人才而言，书籍与期刊起着特殊重要的作用．许多成就卓越的数学家在青年时代都曾钻研或参考过一些优秀书籍，从中汲取营养，获得教益．

20 世纪 70 年代后期，我国的数学研究与数学书刊的出版由于文化大革命的浩劫已经破坏与中断了 10 余年，而在这期间国际上数学研究却在迅猛地发展着．1978 年以后，我国青年学子重新获得了学习、钻研与深造的机会．当时他们的参考书籍大多还是 50 年代甚至更早期的著述．据此，科学出版社陆续推出了多套数学丛书，其中《纯粹数学与应用数学专著》丛书与《现代数学基础丛书》更为突出，前者出版约 40 卷，后者则逾 80 卷．它们质量甚高，影响颇大，对我国数学研究、交流与人才培养发挥了显著效用．

《现代数学基础丛书》的宗旨是面向大学数学专业的高年级学生、研究生以及青年学者，针对一些重要的数学领域与研究方向，作较系统的介绍．既注意该领域的基础知识，又反映其新发展，力求深入浅出，简明扼要，注重创新．

近年来，数学在各门科学、高新技术、经济、管理等方面取得了更加广泛与深入的应用，还形成了一些交叉学科．我们希望这套丛书的内容由基础数学拓展到应用数学、计算数学以及数学交叉学科的各个领域．

这套丛书得到了许多数学家长期的大力支持，编辑人员也为其付出了艰辛的劳动．它获得了广大读者的喜爱．我们诚挚地希望大家更加关心与支持它的发展，使它越办越好，为我国数学研究与教育水平的进一步提高做出贡献．

杨　乐

2003 年 8 月

前　　言

本书分上下两册. 上册介绍了有限 p 群的基本理论和方法、我国学者在 p 群领域的早期工作、p 群的计数以及交换性较强的几类重要 p 群的分类. 下册分 5 章.

第 10 章继续从不同的角度研究交换性 “较强” 的有限 p 群. 我们观察到, 内交换 p 群的导群的阶是 p, 反之不然. 另外, 内交换 p 群的真子群的导群是平凡的. 由这些观察出发, 导群 p 阶的 p 群、二元生成导群循环的 p 群、真子群的导群的阶不超过 p 的 p 群等被研究和分类. 另外, 对于非交换 p 群, 考虑非交换元生成 p^3, p^4 阶的内交换子群、非交换子群的中心均相等等条件, 这样的 p 群也被分类. 本章介绍这些结果.

第 11 章介绍正规性 “较强” 的有限 p 群. 研究正规性 “较强” 的 p 群, 人们主要从以下三个角度考虑: 一是对非正规子群加以某种限制. 这方面的一个重要结果是 Passman 给出的非正规子群均循环的 p 群的分类. 之后, 非正规子群均同阶、非正规子群的阶不超过 p^2, p^3 的 p 群分别被分类. 二是对非正规子群的正规闭包加以某种限制, 例如, 非正规子群的正规闭包均同阶、非正规子群的正规闭包均包含导群、非正规子群的正规闭包较小等, 这样的 p 群也被研究和分类. 三是研究非正规子群的正规化子较小的 p 群. 再就是弱化正规性条件, 例如, 每个子群为共轭置换子群、TI 子群的 p 群分别被研究和分类. 另外, 还有 Hamilton p 群的其他一些推广. 本章介绍这方面的结果.

第 12 章专门介绍亚 Hamilton p 群的分类. 所谓亚 Hamilton p 群, 就是子群或交换或正规的非交换有限 p 群. 容易看出, Hamilton p 群、内交换 p 群及前几章介绍的 $\mathcal{A}_2$ 群、非正规子群均循环的 p 群、非正规子群的阶不超过 p^2 的 p 群等均是亚 Hamilton p 群. 因而它既可看作交换性较强, 也可看作正规性较强的非交换 p 群. 分类亚 Hamilton p 群也是 p 群中的一个老问题. 安立坚在其北京大学博士学位论文中彻底完成了其同构分类. 本章给予专门介绍.

第 13 章介绍几类临界 p 群的分类. 所谓临界群就是群 G 本身不具有性质 $\mathcal{P}$, 但它的每个真子群 (真商群、截段) 具有性质 $\mathcal{P}$ 的群. 当 G 为 p 群时, 也称之为临界 p 群. 例如, 内交换 p 群、内亚循环 p 群、极小非正则 p 群等都是临界 p 群. 本章介绍另外三类临界 p 群的分类, 即极小非 3 交换 3 群、极小非 $\mathcal{P}_2$-p 群以及内 $\mathcal{P}_2$-p 群. p 交换 p 群是有限 p 群中 “接近” 交换群的一个重要群类. 例如, 当 $p=2$ 时, 2 交换 2 群即为交换群. 另外, 幂零类为 1 的群恰是交换群. 因而幂零类为 2 的 p 群也可看作是 “接近” 交换群的 p 群. 显然, 内类 2 的 p 群的分类可看作是内交

换 p 群分类的一个自然的、较大的推广.

第 14 章介绍我国学者在 p 群其他方面取得的结果. 我们知道, p 群有太多问题是未知的, 从不同角度探索 p 群结构是有益的. 本章的内容主要有 p 群的幂结构、余次数、特征标的核、子群交、Wielandt 子群等问题的研究结果, 以及拟 NC 群、平衡 p 群、自对偶 p 群、特殊类型的 p 群、子群具有某种特定性质的 p 群的分类等结果的介绍.

本书是为具有 p 群初等知识的读者编写的, 在 p 群知识上力图做到自包含. 另外, 对于不以英文发表的文献或不易找到的文献, 都列出了它在 MathSciNet 数据库中的编号, 以方便读者查阅该文的摘要. 再者, 在引用前述结果时, 都按章节统一编号. 例如, 命题 1.1.3 指的是第 1 章第 1 节的第 3 个命题.

由于作者水平有限, 缺陷与不足之处在所难免, 热忱欢迎读者批评指正.

张勤海　安立坚
2016 年 9 月于山西师范大学

目　录

《现代数学基础丛书》序

前言

第 10 章　交换性较强的有限 p 群 ······ 1

10.1　导群 p 阶的 p 群 ······ 1

10.2　二元生成导群循环的 p 群 ······ 3

10.3　真子群的导群至多 p 阶的 p 群 ······ 17

10.4　非亚循环的真子群均为 D_1 群的 p 群 ······ 22

10.5　两个非交换元生成 p^3 阶子群的 p 群 ······ 33

10.6　两个非交换元生成 p^4 阶内交换子群的 p 群 ······ 36

10.7　非交换子群的中心均相等的 p 群 ······ 47

第 11 章　正规性较强的有限 p 群 ······ 55

11.1　非正规子群均循环的 p 群 ······ 56

11.2　非正规子群均同阶的 p 群 ······ 60

11.3　非正规子群的阶至多为 p^2 的 p 群 ······ 65

11.4　非正规子群的阶至多为 p^3 的 p 群 ······ 75

11.5　非正规子群的正规闭包均同阶的 p 群 ······ 82

11.6　非正规子群的正规闭包均包含导群的 p 群 ······ 90

11.7　非正规子群的正规闭包较小的 p 群 ······ 101

11.7.1　$\mathrm{BI}(p)$ 群 ······ 101

11.7.2　$\mathrm{BI}(p^2)$ 群 $(p \geqslant 3)$ ······ 104

11.7.3　$\mathrm{BI}(2^2)$ 群 ······ 110

11.8　非正规子群的正规化子较小的 p 群 ······ 118

11.8.1　非正规子群在其正规化子中的指数为 p 的 p 群 ······ 119

11.8.2　非正规子群在其正规化子中的指数不超过 p^2 的 p 群 ······ 123

11.8.3　非正规子群在其正规化子中的指数为 $p^i(i \geqslant 3)$ 的 p 群 ······ 126

11.8.4　非正规子群在其正规化子中的商群循环的 p 群 ······ 128

11.9　非正规子群生成真子群的 p 群 ······ 131

11.10　循环子群或正规或正规化所有子群的 p 群 ······ 134

11.11　交换子群均为 TI 子群的 p 群 ······ 138

11.12　子群均共轭置换的 p 群 ······ 141

11.13 奇素数幂阶 J 群的分类 ···· 144
11.13.1 三元生成的素数幂阶 J 群 ···· 144
11.13.2 类 2 的素数幂阶 J 群 ···· 149
第 12 章 有限亚 Hamilton p 群 ···· 154
12.1 亚 Hamilton p 群的性质 ···· 154
12.2 导群初等交换的亚 Hamilton p 群的分类 ···· 162
12.3 导群非初等交换的亚 Hamilton p 群的分类 ···· 169
第 13 章 临界 p 群 ···· 180
13.1 极小非 3 交换 3 群的分类 ···· 181
13.2 极小非 $\mathcal{P}_2$-p 群的分类 ···· 189
13.3 内 $\mathcal{P}_n$-p 群的某些性质 ···· 200
13.4 内 $\mathcal{P}_2$-p 群的分类 ···· 205
13.4.1 $G_3 \cong \mathrm{C}_p$ 的情形 ···· 209
13.4.2 $G_3 \cong \mathrm{C}_p^2$ 的情形 ···· 216
第 14 章 关于有限 p 群的其他结果 ···· 222
14.1 有限 p 群的幂结构 ···· 222
14.2 NC 群与拟 NC 群 ···· 234
14.3 有限 p 群的余次数 ···· 236
14.4 某些正则 p 群的分类及应用 ···· 240
14.4.1 型不变量为 $(e, 1, 1, 1)$ 的正则 p 群的分类 ···· 240
14.4.2 型不变量为 $(1, 1, 1, 1, 1)$ 的正则 p 群的分类 ···· 247
14.4.3 p^5 阶群的分类 $(p \geqslant 5)$ ···· 250
14.5 平衡 p 群与 n 平衡 p 群 ···· 252
14.5.1 二元生成平衡 p 群 ···· 252
14.5.2 n 平衡 p 群 ···· 258
14.6 有限 p 群的特征标的核 ···· 267
14.7 自同构群相同的 2 群的例子 ···· 272
14.8 极大交换子群为软的 p 群 ···· 275
14.9 有限 p 群的子群交 ···· 277
14.9.1 $\mathrm{I}_k(G) \cong \mathrm{C}_{p^{k-1}}$ 的 p 群 ···· 277
14.9.2 $|\mathrm{I}_3(G)| = 4$ 的 2 群 ···· 281
14.9.3 $|\mathrm{I}_{\mathcal{A}_1}(G)| \leqslant p^{n-3}$ 的 p^n 阶群 ···· 284
14.9.4 $\Phi_{N\mathcal{A}_1M}(G) > \Phi(G)$ 的 p 群 ···· 289
14.10 有限自对偶 p 群 ···· 291
14.10.1 有限 s 自对偶 p 群的性质和例子 ···· 292

14.10.2 有限 s 自对偶 p 群的分类 ······ 296
14.11 p 群的 Wielandt 列和 Norm ······ 300
14.12 极大类 p 群的 Wielandt 子群 ······ 310
14.13 非中心元的中心化子较小的 p 群 ······ 316
14.13.1 $|C_G(x):\langle x\rangle|\leqslant p^2$ 的 p 群 ······ 316
14.13.2 $C_G(x)/\langle x\rangle$ 循环的 p 群及其推广 ······ 319
14.13.3 有一个自中心化循环正规子群的 p 群 ······ 329
14.14 两个共轭元生成小阶子群的 p 群 ······ 333
14.15 仅有唯一的某型 p^3 阶内交换子群的 p 群 ······ 338
14.16 具有一类可补正规子群的 p 群 ······ 342
参考文献 ······ 347
索引 ······ 362
《现代数学基础丛书》已出版书目 ······ 363

第 10 章　交换性较强的有限 p 群

前面看到, 最接近交换群的非交换群自然是内交换群, 也称为 $\mathcal{A}_1$ 群. 研究比 $\mathcal{A}_1$ 群类更大的群类被许多群论学家关注, 并取得了基础性的结果. 例如, $\mathcal{A}_2$ 群、$\mathcal{A}_3$ 群的同构分类, 以及具有一个内交换极大子群的 p 群的分类等. 除此之外, 从其他的角度研究内交换群类的推广也有许多成果, 例如, 文献 [1], [35], [36], [182] 研究导群 p 阶的 p 群. 文献 [202], [218] 研究了导群是 (p,p) 型的 p 群. 导群循环的有限 p 群的研究在文献上也可以找到很多论文, 参见 [48], [49], [63], [81], [120], [158], [219] 等. 值得一提的是, Miech[158] 在 1975 年给出了二元生成、导群循环的有限 p 群 $(p>2)$ 的完全分类. 但他使用了过多的参数, 不太好应用. 2013 年, 宋蕾薇在 [209] 中使用文献 [242] 描述的方法, 对这类群重新给出了分类. 该分类比 Miech 在 [158] 给出的分类简单. 对于 $p=2$ 的情形, 这个问题仍未解决. 注意到内交换群的真子群的导群是平凡的. 黎先华等[256, 257] 研究每个真子群的导群均较小的 p 群. Janko 在文献 [102], [104], [106] 中进一步减弱文献 [256] 的条件, 得到了这些 p 群结构的描述. 张勤海等[265] 进一步研究真子群亚循环或真子群的导群的阶不超过 p 的 p 群. 安立坚等[7]、张勤海等[274] 则从两个非交换元生成较小阶的内交换群的角度研究交换性较强的 p 群. 总之, 研究交换性较强或较好的 p 群是 p 群领域的活跃课题. 本节介绍该领域的有关结果.

10.1　导群 p 阶的 p 群

导群 p 阶的有限 p 群的结构可由中心积描述.

引理 10.1.1　设 G 是有限 p 群且 $|G'|=p$, H 是 G 的内交换子群. 则 $G=H*C_G(H)$.

证明　由定理 1.7.7 可知 $d(H)=2$. 不妨设 $H=\langle a,b\rangle$. 则 $C_G(H)=C_G(a)\bigcap C_G(b)$. 考虑 a 在 G 中的共轭类, 则

$$a^G=\{a^g \mid g\in G\}=\{a[a,g] \mid g\in G\}\subseteq aG'.$$

因为 $|G'|=p$, 故 $|a^G|\leqslant p$. 从而 $|a^G|=p$, 即 $|G:C_G(a)|=p$. 同理 $|G:C_G(b)|=p$. 于是 $|G:C_G(H)|=p^2$. 现在有

$$|HC_G(H)|=\frac{|H||C_G(H)|}{|H\bigcap C_G(H)|}=\frac{|H||C_G(H)|}{|Z(H)|}.$$

因为 H 内交换, 再由定理 1.7.7 可知 $|H:Z(H)|=p^2$. 于是 $|HC_G(H)|=|G|$. □

定理 10.1.2 设 G 是有限 p 群且 $|G'|=p$. 则

(1) 存在 G 的内交换子群 $A_1,A_2,\cdots,A_s$ 使得 $G=(A_1*A_2*\cdots*A_s)Z(G)$;

(2) $G/Z(G)$ 是 p^{2s} 阶的初等交换群, 记为 $\mathrm{E}_{p^{2s}}$;

(3) 若 G/G' 初等交换, 则对 $1\leqslant i\leqslant s$ 均有 $|A_i|=p^3$, $A_1*A_2*\cdots*A_s$ 为超特殊 p 群.

证明 (1) 对 G 作归纳. 设 A_1 是 G 的内交换子群. 由引理 10.1.1, 即得 $G=A_1*C_G(A_1)$. 令 $C=C_G(A_1)$. 若 C 交换, 则 $G=A_1Z(G)$. 若 C 不交换, 则 $|C'|=p$. 由归纳假设, 对于群 C 定理成立. 不妨设

$$C=(A_2*A_3*\cdots*A_s)Z(C),$$

其中 $A_2,A_3,\cdots,A_s$ 是内交换子群. 明显地, $Z(C)=Z(G)$.

(2) 对 s 进行归纳. 当 $s=1$ 时, $G=A_1Z(G)$. 于是

$$G/Z(G)=A_1Z(G)/Z(G)\cong A_1/(A_1\bigcap Z(G))=A_1/Z(A_1)=A_1/\Phi(A_1)\cong \mathrm{E}_{p^2}.$$

结论成立. 当 $s\geqslant 2$ 时, 设 $G=A_1*N_1$, 其中 $N_1=(A_2*\cdots*A_s)Z(G)$. 下证

$$G/Z(G)=A_1Z(G)/Z(G)\times N_1/Z(G).$$

因为 $Z(G)=Z(N_1)$, 由归纳假设可知

$$N_1/Z(N_1)=N_1/Z(G)\cong \mathrm{E}_{p^{2(s-1)}}.$$

又因为 $Z(G)=Z(N_1)\leqslant N_1$, 由模律可得 $A_1Z(G)\bigcap N_1=(A_1\bigcap N_1)Z(G)$. 又 $A_1\bigcap N_1\leqslant Z(G)$, 于是 $A_1Z(G)\bigcap N_1\leqslant Z(G)$. 从而

$$G/Z(G)=A_1Z(G)/Z(G)\times N_1/Z(G)\cong \mathrm{E}_{p^2}\times \mathrm{E}_{p^{2(s-1)}}\cong \mathrm{E}_{p^{2s}}.$$

(3) 由于 $1\neq A_i'\leqslant G'$, 故 $G'=A_i'$ 对所有的 $1\leqslant i\leqslant s$. 又 G/G' 初等交换, 故

$$A_iG'/G'\cong A_i/G'\bigcap A_i=A_i/A_i'$$

初等交换. 从而 $\Phi(A_i)=A_i'$. 因为 $d(A_i)=2$, 于是 $|A_i/\Phi(A_i)|=p^2$. 由此可得 $|A_i|=p^3$ 对所有的 $1\leqslant i\leqslant s$.

令 $K=A_1*A_2*\cdots*A_s$, 其中 $A_i=\langle a_i,b_i\rangle$. 由归纳法可证

$$K/G'=\langle\bar{a}_1\rangle\times\langle\bar{b}_1\rangle\times\langle\bar{a}_2\rangle\times\langle\bar{b}_2\rangle\times\cdots\times\langle\bar{a}_s\rangle\times\langle\bar{b}_s\rangle,$$

任取 $k\in K$, 则

$$\bar{k}=\bar{a}_1^{x_1}\bar{b}_1^{y_1}\bar{a}_2^{x_2}\bar{b}_2^{y_2}\cdots\bar{a}_s^{x_s}\bar{b}_s^{y_s}.$$

因为 K/G' 初等交换, 故 $0\leqslant x_i,y_i\leqslant p-1$. 从而存在 $z\in G'$ 使得

$$k=a_1^{x_1}b_1^{y_1}a_2^{x_2}b_2^{y_2}\cdots a_s^{x_s}b_s^{y_s}z.$$

由于 $K=A_1*A_2*\cdots*A_s$ 是中心积, 故 $[k,a_i]=[b_i^{y_i},a_i]$ 且 $[k,b_i]=[a_i^{x_i},b_i]$. 显然, 对于 $1\leqslant x_i,y_i\leqslant p-1$, 有

$$A_i=\langle a_i,b_i\rangle=\langle a_i^{x_i},b_i\rangle=\langle a_i,b_i^{y_i}\rangle$$

内交换. 故 $1\neq[a_i,b_i]=[b_i^{y_i},a_i]=[a_i,b_i^{y_i}]$. 由此可得 $\forall i$, $[k,a_i]=1\Leftrightarrow y_i=0$ 和 $[k,b_i]=1\Leftrightarrow x_i=0$. 由此进一步可得, $k\in Z(K)$ 当且仅当 $x_i=y_i=0,\forall i$. 故 $k=z\in G'$. 所以 $Z(K)\leqslant G'$. 因为 $1<|Z(K)|$, 所以 $Z(K)=G'$. 由 (1) 可知, $Z(G)=Z(K)$. 显然 $G'=K'$. 另一方面, $\Phi(K)\leqslant\Phi(G)$. 由 G/G' 初等交换得 $\Phi(G)=G'$. 故 $\Phi(K)=K'$. 由此可知 $Z(K)=\Phi(K)=K'$ 且阶为 p. 故 $K=A_1*A_2*\cdots*A_s$ 是超特殊 p 群. □

注 张勤海等在文献 [272] 给出了超特殊 p 群的三个等价性质.

10.2 二元生成导群循环的 p 群

本节介绍文献 [209] 获得的导群循环二元生成的有限 p 群 $(p>2)$ 的分类结果.

命题 10.2.1 设 G 是有限正则 p 群, $H\trianglelefteq G$. 则 $\omega(G/H)+\omega(H)\geqslant\omega(G)$.

证明 因为

$$|G/\mho_1(G)|=p^{\omega(G)},\quad p^{\omega(G/H)}=|(G/H)/\mho_1(G/H)|=|G/\mho_1(G)H|,$$

有 $|\mho_1(G)H/\mho_1(G)|=p^{\omega(G)-\omega(G/H)}$. 注意到

$$\mho_1(G)H/\mho_1(G)\cong H/\mho_1(G)\bigcap H,\quad \mho_1(H)\leqslant\mho_1(G)\bigcap H.$$

由此可得

$$p^{\omega(G)-\omega(G/H)}=|\mho_1(G)H/\mho_1(G)|=|H/\mho_1(G)\bigcap H|\leqslant|H/\mho_1(H)|=p^{\omega(H)}.$$

因而 $\omega(G)-\omega(G/H)\leqslant\omega(H)$. 故 $\omega(G/H)+\omega(H)\geqslant\omega(G)$. □

定理 10.2.2 设 G 为二元生成的有限 p 群, G' 循环, p 为奇素数. 则 G 正则且 $\omega(G)\leqslant 3$.

证明　由于 $p>2$ 且 G' 循环, 因此由定理 1.11.4(3) 可知, G 正则. 进一步, 由于 G' 循环, 因此 $G''=1$. 故 $\Phi(G')=\mho_1(G')$. 因而

$$p^{\omega(G')}=|G'/\mho_1(G')|=|G'/\Phi(G')|=p.$$

故 $\omega(G')=1$. 接下来, 因为

$$p^{\omega(G/G')}=|G/G'/\mho_1(G/G')|=|G/\mho_1(G)G'|=|G/\Phi(G)|=p^2,$$

所以 $\omega(G/G')=2$. 因而由命题 10.2.1 知, $\omega(G)\leqslant\omega(G')+\omega(G/G')=3$. □

由于 $d(G)=2$ 且 $d(G)\leqslant\omega(G)$, 因此 $\omega(G)=2$ 或 3. 若 $\omega(G)=2$, 由定理 7.2.1 可知 G 亚循环. 而亚循环 p 群已被分类. 故下面仅考虑 $\omega(G)=3$ 的情形. 因为 G 正则且 $p^3=p^{\omega(G)}=|G/\mho_1(G)|$, 因此可设 G 的型不变量为 (n,m,r). 显然, $\exp(G)=p^n$ 且 $n\geqslant m\geqslant r$. 任取 G 的一个 L 群列

$$G=L_0(G)>L_1(G)>L_2(G)>L_3(G)=\mho_1(G).$$

由于 $|G/L_2(G)|=p^2$, 因此 $G'\leqslant L_2(G)$. 显然 $\mho_1(G)\leqslant L_2(G)$. 故 $\Phi(G)\leqslant L_2(G)$. 又因 $d(G)=2$, 所以 $|G/\Phi(G)|=p^2$. 故总可假设 $L_2(G)=\Phi(G)$.

取 $a\in L_0(G)\backslash L_1(G)$, $b\in L_1(G)\backslash L_2(G)$, $d\in L_2(G)\backslash L_3(G)$ 且为最小阶元素. 由定理 4.2.17 可知, (a,b,d) 为一组唯一性基底, 其中 $o(a)=p^n$, $o(b)=p^m$, $o(d)=p^r$ 且 $G=\langle a,b\rangle$. 由于 G' 循环, 因此总可假设 $G'=\langle c\rangle$ 且 $o(c)=p^u$. 容易证明 $c\in L_2(G)\backslash L_3(G)$. 由于 $G'=\langle c\rangle=\langle[a,b]\rangle$ 且 G 正则, 由定理 1.11.5(5) 可知 $u\leqslant m$. 故 $n\geqslant m\geqslant u\geqslant r$.

下面分 $u=r$ 和 $u>r$ 两种情形对导群循环二元生成的有限 p 群进行分类.

先看 $u=r$ 的情形.

定理 10.2.3　设 G 为二元生成导群循环的奇阶有限 p 群, 且设 G 的型不变量为 (n,m,r), $|G'|=p^r$. 则

$$G=\langle a,b,c\mid a^{p^n}=b^{p^m}=c^{p^r}=1,[a,b]=c,[c,a]=c^{p^s},[c,b]=c^{p^t}\rangle,$$

其中 n,m,r,s,t 为正整数, $r\leqslant m\leqslant n$, $s\leqslant t=r$ 或者 $r\leqslant m<n$, $s\leqslant t<\min\{r,n-m+s\}$, 且对于参数 n,m,r,s,t 的不同取值, 对应的群互不同构.

证明　注意到 $|G'|=p^r$, 因此 (a,b,c) 为 G 的一组唯一性基底. 显然

$$\langle a\rangle\bigcap\langle b\rangle=\langle a\rangle\bigcap\langle c\rangle=\langle b\rangle\bigcap\langle c\rangle=1.$$

考虑群 $\langle a,c\rangle$ 和 $\langle b,c\rangle$. 因为 $\langle c\rangle\trianglelefteq G$, 所以 $\langle a,c\rangle$, $\langle b,c\rangle$ 均为亚循环 p 群. 由定理 2.1.6, 分别用 a, b 的适当方幂替换 a,b 可得

$$a^{p^n}=b^{p^m}=c^{p^r}=1,\quad a^{-1}ca=c^{1+p^s},\quad b^{-1}cb=c^{1+p^t},$$

其中 n, m, r, s, t 为正整数且 $s, t \leqslant r$. 由于 $G' = \langle [a, b] \rangle = \langle c \rangle$, 因此不妨设 $[a, b] = c$.

若 $s > t$, 由 [247] 中的引理 6.2.3 知, 可取适当的 i 并用 ab^i 替换 a 可得 $(ab^i)^{-1}c(ab^i) = c^{1+p^t}$. 进而总可设 $s \leqslant t$.

若 $\langle b, c \rangle$ 交换, 则可得定理中的群, 此为 $r \leqslant m \leqslant n$, $s \leqslant t = r$ 的情形. 若 $\langle b, c \rangle$ 非交换. 断言 $t < n - m + s$. 若否, 则 $t \geqslant n - m + s$. 由 [247] 中的引理 6.2.3 知, 可取适当的 i, 并用 $a^{ip^{n-m}}b$ 替换 b 可得

$$(a^{ip^{n-m}}b)^{-1}c(a^{ip^{n-m}}b) = c, \quad o(a^{ip^{n-m}}b) = p^m.$$

并且 $(a, a^{ip^{n-m}}b, c)$ 仍为 G 的一组唯一性基底. 由于 $s \leqslant t < n - m + s$, 因此 $n > m$. 从而可得定理中的群, 此为 $r \leqslant m < n$, $s \leqslant t < \min\{r, n - m + s\}$ 的情形.

下面将证明定理中所有参数均是 G 的不变量. 由于 G 的型不变量为 (n, m, r) 且 $|G_3| = p^{r-s}$, 因此 n, m, r, s 为不变量. 最后我们来证明 t 也是不变量. 显然只需考虑 $r \leqslant m < n$, $s \leqslant t < \min\{r, n - m + s\}$ 的情形. 不失一般性, 令

$$a_1 = a^{i_1}b^{j_1}c^{k_1}, \quad b_1 = a^{i_2p^{n-m}}b^{j_2}c^{k_2}, \quad c_1 = [a_1, b_1],$$

其中 $p \nmid i_1j_2$. 经计算知 $b_1^{-1}c_1b_1 = c_1^{(1+p^s)^{i_2p^{n-m}}(1+p^t)^{j_2}}$. 由于 $t < n - m + s$ 且 $p \nmid j_2$, 因此可记 $b_1^{-1}c_1b_1 = c_1^{(1+wp^t)}$, 其中 $p \nmid w$. 故 t 是不变量.

综上可知, 参数 n, m, r, s, t 均为不变量. 因此, 对于参数 n, m, r, s, t 的不同取值, 对应的群互不同构.

最后, 利用循环扩张理论可以证明, 对于定理中得到的群而言, $|G| = p^{n+m+r}$, 并且通过计算可知 G' 循环且 G 的型不变量为 (n, m, r). □

下面处理 $u > r$ 的情形.

定理 10.2.4 设 G 为二元生成导群循环的奇阶有限 p 群, 其型不变量为 (n, m, r). 再设 $|G'| = p^u$. 则 G 同构于以下群之一, 这里 $n, m, u, r, s, t, \theta, i, \sigma$ 均为正整数.

(Ⅰ) $\langle a, b, c \mid a^{p^{n-u+r}} = c^{p^r}, b^{p^m} = c^{p^u} = 1, [a, b] = c, [c, a] = c^{p^s}, [c, b] = 1 \rangle$, 其中 $r + 1 \leqslant u \leqslant m \leqslant n$, $u - r \leqslant s \leqslant u \leqslant n - u + r$.

(Ⅱ) $\langle a, b, c \mid a^{p^{n-u+r}} = c^{p^r}, b^{p^m} = c^{p^u} = 1, [a, b] = c^\sigma, [c, a] = 1, [c, b] = c^{p^t} \rangle$, 其中 $r + 1 \leqslant u \leqslant m \leqslant n$, $u - (r + m - \min\{m, n - u + r\}) \leqslant t < u$, $p \nmid \sigma$ 且 $\sigma \leqslant \min\{p^{u-r}, p^{u-t}\}$. 当 $n - u + r \geqslant u$ 时, $u - r \leqslant t$. 当 $n - u + r < u$ 时, $\sigma \equiv 1 (\mathrm{mod}\ p^{u-r-t})$ 且 $n - u = t$.

(Ⅲ) $\langle a, b, c \mid a^{p^{n-u+r}} = c^{p^r}, b^{p^m} = c^{p^u} = 1, [a, b] = c^\sigma, [c, a] = c^{p^s}, [c, b] = c^{p^t} \rangle$, 其中 $r + 1 \leqslant u \leqslant m \leqslant n$, $t < \min\{n - m + s, u\}$, $u - r \leqslant s < \min\{m - \min\{m, n - u + r\} + t, u\}$, $p \nmid \sigma$ 且 $\sigma \leqslant \min\{p^{u-r}, p^{\min\{n-m+s,u\}-t}\}$. 当 $n - u + r \geqslant u$ 时, $u - r \leqslant t$. 当 $n - u + r < u$ 时, $\sigma \equiv 1 (\mathrm{mod}\ p^{u-r-t})$ 且 $n - u = t$.

(Ⅳ) $\langle a,b,c \mid a^{p^{n-u+r+\theta}}=c^{p^{r+\theta}}, b^{p^{m-\theta}}=c^{p^r}, c^{p^u}=1, [a,b]=c^\sigma, [c,a]=c^{p^s}, [c,b]=1\rangle$, 其中 $r+1\leqslant u\leqslant m<n-u+r+\theta$, $\theta\leqslant u-r$, $\theta<m-r$, $u-r-\theta\leqslant s\leqslant u$, $p\nmid\sigma$, $\sigma p^{m-\theta}+p^{r+s}\equiv 0(\mathrm{mod}\ p^u)$. 并且若 $n-u+r+\theta-m+\theta\geqslant u-s$, 则 $\sigma\leqslant\min\{p^\theta,p^{u-s}\}$. 若 $n-u+r+\theta-m+\theta<u-s$, 则 $\sigma\leqslant\min\{p^{\theta+u-s-(n-u+r+\theta)+(m-\theta)},p^{u-r}\}$.

(Ⅴ) $\langle a,b,c\mid a^{p^{n-u+r+\theta}}=c^{p^{r+\theta}}, b^{p^{m-\theta}}=c^{p^r}, c^{p^u}=1, [a,b]=c^\sigma, [c,a]=1, [c,b]=c^{p^t}\rangle$, 其中 $r+1\leqslant u\leqslant m<n-u+r+\theta$, $\theta\leqslant\min\{u-r,m-u\}$, $u-r\leqslant t<u$, $p\nmid\sigma$ 且 $\sigma\leqslant\min\{p^{u-r-\theta},p^{u-t}\}$.

(Ⅵ) $\langle a,b,c\mid a^{p^{n-u+r+\theta}}=c^{ip^{r+\theta}}, b^{p^{m-\theta}}=c^{p^r}, c^{p^u}=1, [a,b]=c^\sigma, [c,a]=c^{p^s}, [c,b]=c^{p^t}\rangle$, 其中 $r+1\leqslant u\leqslant m<n-u+r+\theta$, $\theta\leqslant u-r$, $\theta<m-r$, $u-r-\theta\leqslant s<t$, $u-r\leqslant t<\min\{u,n-u+r+\theta-m+\theta+s\}$, $p\nmid i\sigma$, $\sigma p^{m-\theta}+p^{r+s}\equiv 0(\mathrm{mod}\ p^u)$, $\sigma\leqslant\min\{p^\theta,p^{t-s}\}$ 并且 $i\leqslant\min\{p^{u-t},p^{u-r-\theta}\}$.

并且不同类型的群或者相同类型但不同参数的群互不同构.

证明　注意到, (a,b,d) 为 G 的一组唯一性基底且 $G'=\langle c\rangle$, $o(c)=p^u$ 其中 $u>r$. 因为 $\langle a\rangle\bigcap\langle b\rangle=1$, 断言 $\langle a\rangle\bigcap\langle c\rangle$, $\langle b\rangle\bigcap\langle c\rangle$ 中至少有一个为 1. 若否, 则可设

$$\langle a\rangle\bigcap\langle c\rangle=\langle c^{p^\alpha}\rangle,\quad \langle b\rangle\bigcap\langle c\rangle=\langle c^{p^\beta}\rangle.$$

故 $1\neq\langle c^{p^{\max\{\alpha,\beta\}}}\rangle\leqslant\langle a\rangle\bigcap\langle b\rangle$, 矛盾. 不妨设 $\langle b\rangle\bigcap\langle c\rangle=1$ 且 $\langle a\rangle\bigcap\langle c\rangle=\langle c^{p^\alpha}\rangle$. 则 $o(\bar a)=p^{n-u+\alpha}$. 由于 $\langle b\rangle\bigcap\langle c\rangle=1$, 因此 $o(\bar b)=p^m$. 设 $|\langle\bar a\rangle\bigcap\langle\bar b\rangle|=p^\theta$. 由于

$$p^{n+m+r}=|G|=|\overline{G}||G'|=\frac{p^{n-u+\alpha}p^m}{p^\theta}p^u=p^{n+m+\alpha-\theta},$$

因此 $\alpha=r+\theta$ 且 $o(\bar a)=p^{n-u+r+\theta}$. 进而, 我们分以下两种情形讨论.

情形 1　总存在 G 的一组唯一性基底 (a,b,d) 使得 $\overline{G}=\langle\bar a\rangle\times\langle\bar b\rangle$, 即 $\theta=0$.

显然 $o(\bar a)=p^{n-u+r}$, $o(\bar b)=p^m$ 且 $\langle a^{p^{n-u+r}}\rangle=\langle c^{p^r}\rangle$. 由于 $\langle c\rangle\trianglelefteq G$, 因此 $\langle a,c\rangle$, $\langle b,c\rangle$ 均为亚循环 p 群. 由定理 2.1.6 知, 总可用 a, b 的适当方幂替换 a,b 可得

$$a^{p^{n-u+r}}=c^{p^r},\quad b^{p^m}=c^{p^u}=1,\quad a^{-1}ca=c^{1+p^s},\quad b^{-1}cb=c^{1+p^t},$$

其中 n,m,u,r,s,t 为正整数且 $s,t\leqslant u$. 由于 G' 循环, 因此总可假设 $[a,b]=c^\sigma$, 其中 $p\nmid\sigma$. 进一步, 因为 G 正则, 由定理 1.11.5 可知 $r+s\geqslant u$.

由于 G' 循环, 因此 G 亚交换. 由命题 1.1.9 和命题 1.1.10 知

$$[a^{p^{n-u+r}},b]=c^{\sigma\left(p^{n-u+r}+\sum_{k=2}^{p^{n-u+r}}\binom{p^{n-u+r}}{k}p^{s(k-1)}\right)}.$$

注意到 $r+s\geqslant u$, 因此 $[a^{p^{n-u+r}},b]=c^{\sigma p^{n-u+r}}$. 另一方面, $[a^{p^{n-u+r}},b]=[c^{p^r},b]=c^{p^{r+t}}$. 因此 $\sigma p^{n-u+r}\equiv p^{r+t}(\mathrm{mod}\ p^u)$. 进一步, 若 $n-u+r\geqslant u$, 则 $r+t\geqslant u$. 若 $n-u+r<u$, 则 $n-u=t$ 且 $\sigma\equiv 1(\mathrm{mod}\ p^{u-r-t})$.

子情形 1.1 $\langle b,c\rangle$ 交换.

因为 $t=u$ 且 $\sigma p^{n-u+r}\equiv p^{r+t}(\mathrm{mod}\ p^u)$, 故 $n-u+r\geqslant u$. 令 $b_1=b^{\tau}$, 其中 $\sigma\tau\equiv 1(\mathrm{mod}\ p^u)$. 则 $[a,b_1]=c$ 且 $[c,b_1]=1$. 故 G 同构于定理中的群 (I). 此时, n,m,u,r 为不变量. 进一步, 因为 $|G_3|=p^{u-s}$, 所以 s 为不变量. 因此对于满足定理中条件的参数 n,m,u,r,s 的不同取值, 得到的群互不同构.

子情形 1.2 $\langle b,c\rangle$ 非交换.

类似定理 10.2.3 的讨论, 可得 $t<n-m+s$ 且

$$\begin{cases} s\leqslant t, & n-u+r\geqslant m,\\ s\leqslant m-(n-u+r)+t, & n-u+r<m.\end{cases}$$

从而 $t<\min\{n-m+s,u\}$ 且 $s\leqslant\min\{m-\min\{m,n-u+r\}+t,u\}$.

子情形 1.2.1 $s=\min\{m-\min\{m,n-u+r\}+t,u\}$.

注意到 $r+s\geqslant u$. 因此 $r+m-\min\{m,n-u+r\}+t\geqslant u$. 若 $s=u$, 则 $[c,a]=1$. 若 $s=m-\min\{m,n-u+r\}+t$, 则存在适当的 j 并用 $ab^{jp^{m-\min\{m,n-u+r\}}}$ 替换 a 可得

$$(ab^{jp^{m-\min\{m,n-u+r\}}})^{-1}c(ab^{jp^{m-\min\{m,n-u+r\}}})=c.$$

从而可设 $\langle a,c\rangle$ 交换. 进而 G 有如下定义关系:

$$a^{p^{n-u+r}}=c^{p^r},\quad b^{p^m}=c^{p^u}=1,\quad [a,b]=c^{\sigma},\quad [c,a]=1,\quad [c,b]=c^{p^t},$$

其中

$$r+1\leqslant u\leqslant m\leqslant n,\quad u-(r+m-\min\{m,n-u+r\})\leqslant t<u,\quad p\nmid\sigma,$$

且 σ 为正整数.

因为 G 的型不变量为 (n,m,r), $|G'|=p^u$ 且 $|G_3|=p^{u-t}$, 故 n,m,u,r,t 均为不变量. 从而只需考虑当 σ 取何值时, 对应的群两两互不同构即可. 为方便证明, 用 $G(\sigma)$ 记群 G. 假设 $G(\sigma)\cong G(\sigma')$. 在群 $G(\sigma)$ 中, 令

$$a_1=a^{i_1}b^{j_1}c^{k_1},\quad b_1=a^{i_2}b^{j_2}c^{k_2},\quad c_1=c^{v},$$

其中 $i_1,i_2,j_1,j_2,k_1,k_2,v$ 取适当的整数且 $p\nmid i_1j_2v$ 使得 a_1, b_1 生成 $G(\sigma)$, 且 a_1, b_1, $c_1^{\sigma'}=[a_1,b_1]$ 满足群 $G(\sigma')$ 的定义关系. 显然 $p^{m-\min\{m,n-u+r\}}\mid j_1$ 且 $p^{n-m}\mid i_2$.

经计算知,

$$\begin{cases} (i_1+k_1p^{n-u})p^r \equiv vp^r (\bmod\ p^u), & (10.1)\\ \sigma i_1\dfrac{(1+p^t)^{j_2}-1}{p^t}(1+p^t)^{j_1}-\sigma i_2\dfrac{(1+p^t)^{j_1}-1}{p^t}(1+p^t)^{j_2} & \\ \quad +k_1[(1+p^t)^{j_2}-1]+k_2[1-(1+p^t)^{j_1}]=v\sigma', & (10.2)\\ (1+p^t)^{j_1}\equiv 1(\bmod\ p^u), & (10.3)\\ (1+p^t)^{j_2-1}\equiv 1(\bmod\ p^u). & (10.4)\end{cases}$$

由式 (10.3), (10.4) 可知 $p^{u-t}\mid j_1$ 且 $p^{u-t}\mid j_2-1$. 用 $\sigma'\times(10.1)$ 得

$$\sigma'(i_1+k_1p^{n-u})p^r\equiv v\sigma' p^r(\bmod\ p^u).$$

进而根据式 (10.2) 可知, $\sigma' i_1\equiv \sigma i_1 j_2-\sigma i_2 j_1(\bmod\ p^{u-r})$. 因此

$$\sigma\equiv\sigma'(\bmod\ \min\{p^{u-r},p^{u-t}\}).$$

下证总可取适当的元素满足前面的定义关系且使得 $\sigma\leqslant\min\{p^{u-r},p^{u-t}\}$. 令 $a'=a, b'=b^j, c'=c^v$, 其中 $v\equiv 1(\bmod\ p^{u-r})$, $j\equiv 1(\bmod\ p^{u-t})$. 经计算知

$$[a',b']=c^{\sigma(j+\binom{j}{2}p^t+\cdots+p^{t(j-1)})}.$$

容易证明: 总存在适当的 $j=j_0$ 使得

$$\sigma\left(j+\binom{j}{2}p^t+\cdots+p^{t(j-1)}\right)\leqslant p^{u-t}.$$

若 $p^{u-t}\leqslant p^{u-r}$, 令 $v=1$, 结论得证. 若 $p^{u-t}>p^{u-r}$, 则可取适当的 $v=v_0$, 其中 $v_0\equiv 1(\bmod\ p^{u-r})$ 使得

$$v^{-1}\sigma(j+\binom{j}{2}p^t+\cdots+p^{t(j-1)})\leqslant p^{u-r}.$$

结论亦成立. 从而得定理中的群 (Ⅱ).

子情形 1.2.2　$s<\min\{m-\min\{m,n-u+r\}+t,u\}$.

此时 G 有如下的定义关系:

$$a^{p^{n-u+r}}=c^{p^r},\quad b^{p^m}=c^{p^u}=1,\quad [a,b]=c^\sigma,\quad [c,a]=c^{p^s},\quad [c,b]=c^{p^t},$$

其中

$$r+1\leqslant u\leqslant m\leqslant n,$$

$$t<\min\{n-m+s,u\},$$

$$u-r\leqslant s<\min\{m-\min\{m,n-u+r\}+t,u\},\quad p\nmid\sigma.$$

显然 n,m,r,u 均为 G 的不变量. 进一步, 类似定理 10.2.3 的证明可知, s,t 也是 G 的不变量. 从而我们只需考虑当 σ 取何值时, 对应的群两两互不同构. 为方便证明, 用 $G(\sigma)$ 记群 G. 假设 $G(\sigma)\cong G(\sigma')$. 在群 $G(\sigma)$ 中, 令

$$a_1=a^{i_1}b^{j_1}c^{k_1},\quad b_1=a^{i_2}b^{j_2}c^{k_2},\quad c_1=c^v,$$

其中 $i_1,i_2,j_1,j_2,k_1,k_2,v$ 取适当整数且 $p\nmid i_1j_2v$ 使得 a_1, b_1 生成 $G(\sigma)$, 且 a_1, $b_1,c_1^{\sigma'}=[a_1,b_1]$ 满足群 $G(\sigma')$ 的定义关系. 显然 $p^{m-\min\{m,n-u+r\}}\mid j_1$ 且 $p^{n-m}\mid i_2$.

类似子情形 1.2.1 的证明可得

$$\sigma\equiv\sigma'(\text{mod }\min\{p^{u-r},p^{\min\{n-m+s,u\}-t}\}).$$

进而总可取适当的元素满足前面的定义关系且使得 $\sigma\leqslant\min\{p^{u-r},p^{\min\{n-m+s,u)-t}\}$. 综上可得定理中的群 (III). 类似定理 10.2.3 可证明, 群 (Ⅰ)—(III) 两两互不同构.

情形 2 G 的任意一组唯一性基底 (a,b,d) 均不满足 $\bar G=\langle\bar a\rangle\times\langle\bar b\rangle$, 即 $\theta\neq0$.

由于 $\langle a\rangle\bigcap\langle c\rangle=\langle c^{p^{r+\theta}}\rangle$, $\langle b\rangle\bigcap\langle c\rangle=1$ 且 $|\langle\bar a\rangle\bigcap\langle\bar b\rangle|=p^\theta$, 因此 $\langle\bar a^{p^{n-u+r}}\rangle=\langle\bar b^{p^{m-\theta}}\rangle$. 进而总可设 $\bar a^{p^{n-u+r}}=\bar b^{ip^{m-\theta}}$, 其中 $p\nmid i$. 断言 $o(\bar a)>o(\bar b)$. 若否, 令 $a_1=ab^{-ip^{(m-\theta)-(n-u+r)}}$. 显然 $o(\bar a_1)=p^{n-u+r}$. 由于 $o(\bar b)=p^m$ 且 $|\overline{G}|=p^{n+m+r-u}$, 因此 $\overline{G}=\langle\bar a_1\rangle\times\langle\bar b\rangle$. 易知 $a_1\in L_0(G)\backslash L_1(G)$ 且 $o(a_1)=p^n$. 归结为情形 1.

由于 $o(\bar a)>o(\bar b)$, 因此 $n-u+r+\theta>m$. 令 $b_1=a^{-i^{-1}p^{n-u+r+\theta-m}}b$. 则 $o(\bar b_1)=p^{m-\theta}$. 从而 $\overline{G}=\langle\bar a\rangle\times\langle\bar b_1\rangle$, 其中 $o(\bar a)=p^{n-u+r+\theta}$, $o(\bar b_1)=p^{m-\theta}$. 因为 $\theta\neq0$, 故 b_1 不属于 G 的任意一组唯一性基底.

因为 $\overline{G}$ 交换, 故 $\overline{G}$ 的型不变量为 $(n-u+r+\theta,m-\theta)$. 因此 $n-u+r+\theta,m-\theta$ 均为不变量. 注意到 n,m,u,r 为不变量. 因此 θ 亦为不变量. 注意到 $\bar b_1^{p^{m-\theta}}=1$, 故不失一般性, 可设 $b_1^{p^{m-\theta}}=c^{p^x}$. 易知 G 为 p^m 交换的, 因此 $b_1^{p^m}=a^{-i^{-1}p^{n-u+r+\theta}}$. 由于 $\langle a\rangle\bigcap\langle c\rangle=\langle c^{p^{r+\theta}}\rangle$, 故 $\langle a^{p^{n-u+r+\theta}}\rangle=\langle c^{p^{r+\theta}}\rangle$. 因而总可设 $b_1^{p^m}=c^{jp^{r+\theta}}$, 其中 $p\nmid j$. 故 $jp^{r+\theta}\equiv p^{x+\theta}(\text{mod }p^u)$. 若 $r+\theta\geqslant x+\theta$, 则 $p^{x+\theta}(jp^{r-x}-1)\equiv0(\text{mod }p^u)$. 从而 $x=r$. 若 $r+\theta<x+\theta$, 则 $p^{r+\theta}(j-p^{x-r})\equiv0(\text{mod }p^u)$. 若 $(j-p^{x-r})\equiv0(\text{mod }p^u)$, 则 $x=r$. 若 $(j-p^{x-r})\not\equiv0(\text{mod }p^u)$, 则 $x+\theta>r+\theta\geqslant u$. 因此 $x>r$ 且 $r+\theta=u$. 从而可设 $x=r+\varepsilon$. 故 $b_1^{p^{m-\theta}}=c^{p^{r+\varepsilon}}$ 且 $b_1^{p^{m-\varepsilon}}=1$. 显然 $b_1\in L_1(G)\backslash L_2(G)$. 因此 $o(b_1)\geqslant p^m$, 矛盾. 因而 $x=r$. 故 $b_1^{p^{m-\theta}}=c^{p^r}$. 进而, 用 b 替换 b_1 可得, $b^{p^{m-\theta}}=c^{p^r}$.

由于 $\langle c\rangle\trianglelefteq G$, 因此 $\langle a,c\rangle$ 和 $\langle b,c\rangle$ 均亚循环. 利用定理 2.1.6, 分别用 a, b 的适当方幂替换 a,b 可得

$$a^{p^{n-u+r+\theta}}=c^{ip^{r+\theta}},\quad b^{p^{m-\theta}}=c^{p^r},\quad c^{p^u}=1,\quad a^{-1}ca=c^{1+p^s},\quad b^{-1}cb=c^{1+p^t},$$

其中 n, m, u, r, s, t, θ 为正整数, $s, t \leqslant u$, $\theta \leqslant u-r$ 且 $p \nmid i$. 因为 $G' = \langle [a,b] \rangle = \langle c \rangle$, 所以总可假设 $[a,b] = c^{\sigma}$, 其中 $p \nmid \sigma$.

由于 G 正则, 利用定理 1.11.5 可知, $m-\theta+t \geqslant u$, $r+t \geqslant u$ 且 $r+\theta+s \geqslant u$. 从而 $m \geqslant r+\theta$. 断言 $m > r+\theta$. 若否, 则 $m = u = r+\theta$. 令 $b_1 = bc^{-1}$ 且 $[a, b_1] = c^{\sigma'}$. 则 $b_1^{p^r} = 1$ 且 $b_1^{-1}cb_1 = c^{1+p^t}$. 此时, 显然 $b_1 \in L_1(G) \backslash L_2(G)$, 故 $o(b_1) \geqslant p^m$. 因此 $r = u = m$, 矛盾. 类似情形 1 的证明可得, $\sigma p^{m-\theta} + p^{r+s} \equiv 0 (\mathrm{mod}\ p^u)$.

子情形 2.1 $\langle b, c \rangle$ 交换.

不失一般性, 分别用 b^i 和 c^i 替换 b 和 c 可得

$$a^{p^{n-u+r+\theta}} = c^{p^{r+\theta}}, \quad b^{p^{m-\theta}} = c^{p^r}, \quad c^{p^u} = 1, \quad [a,b] = c^{\sigma}, \quad a^{-1}ca = c^{1+p^s}, \quad b^{-1}cb = c,$$

其中

$$r+1 \leqslant u \leqslant m < n-u+r+\theta, \quad \theta \leqslant u-r, \quad \theta < m-r, \quad u-r-\theta \leqslant s \leqslant u, \quad p \nmid \sigma,$$

且 σ 为正整数. 由于 $|G_3| = p^{u-s}$, 因此 s 为不变量. 从而只需考虑当 σ 取何值时, 对应的群两两互不同构即可. 为方便证明, 用 $G(\sigma)$ 记群 G. 假设 $G(\sigma) \cong G(\sigma')$. 在群 $G(\sigma)$ 中, 令

$$a_1 = a^{i_1} b^{j_1} c^{k_1}, \quad b_1 = a^{i_2} b^{j_2} c^{k_2}, \quad c_1 = c^{v},$$

其中 $i_1, i_2, j_1, j_2, k_1, k_2, v$ 为适当的正整数, 且 $p \nmid i_1 j_2 v$ 使得 a_1, b_1 生成 $G(\sigma)$, 并且 $a_1, b_1, c_1^{\sigma'} = [a_1, b_1]$ 满足 $G(\sigma')$ 的定义关系. 显然 $p^{n-u+r+\theta-m+\theta} \mid i_2$, 从而可记 $i_2 = lp^{n-u+r+\theta-m+\theta}$.

经计算知

$$\begin{cases} i_1 p^{r+\theta} + j_1 p^{r+(n-u+r+\theta)-(m-\theta)} \equiv v p^{r+\theta} (\mathrm{mod}\ p^u), & (10.5) \\ l p^{r+\theta} + j_2 p^r + k_2 p^{m-\theta} \equiv v p^r (\mathrm{mod}\ p^u), & (10.6) \\ \sigma \dfrac{[(1+p^s)^{i_1} - 1] j_2}{p^s} - \sigma \dfrac{[(1+p^s)^{i_2} - 1] j_1}{p^s} & \\ \quad -k_2[(1+p^s)^{i_1} - 1] + k_1[(1+p^s)^{i_2} - 1] = v\sigma', & (10.7) \\ (1+p^s)^{i_1} \equiv 1 + p^s (\mathrm{mod}\ p^u), & (10.8) \\ (1+p^s)^{i_2} \equiv 1 (\mathrm{mod}\ p^u). & (10.9) \end{cases}$$

由式 (10.8) 和 (10.9) 知

$$i_1 \equiv 1 (\mathrm{mod}\ p^{u-s}), \quad i_2 = lp^{n-u+r+\theta-m+\theta} \equiv 0 (\mathrm{mod}\ p^{u-s}).$$

令 $\sigma' \times [(10.6) \times i_1 - (10.5) \times l]$, 则

$$\sigma'(i_1 j_2 - i_2 j_1) p^r + \sigma' i_1 k_2 p^{m-\theta} \equiv v\sigma'(i_1 p^r - l p^{r+\theta}) (\mathrm{mod}\ p^u).$$

故由 (10.7) 可知

$$\sigma'(i_1j_2-i_2j_1)p^r+\sigma' i_1k_2p^{m-\theta}\equiv[\sigma(i_1j_2-i_2j_1)-k_2p^s](i_1p^r-lp^{r+\theta})(\mathrm{mod}\ p^u).$$

由于 $\sigma' p^{m-\theta}+p^{r+s}\equiv 0(\mathrm{mod}\ p^u)$ 且 $r+\theta+s\geqslant u$, 因此 $\sigma' p^r\equiv\sigma i_1p^r-\sigma lp^{r+\theta}(\mathrm{mod}\ p^u)$.

注意到 $i_2=lp^{n-u+r+\theta-m+\theta}\equiv 0(\mathrm{mod}\ p^{u-s})$. 当 $n-u+r+\theta-m+\theta\geqslant u-s$ 时, 由于 $r+\theta\leqslant u$ 且 $i_1\equiv 1(\mathrm{mod}\ p^{u-s})$, 因此 $\sigma'\equiv\sigma(\mathrm{mod}\ \min\{p^\theta,p^{u-s}\})$. 当 $n-u+r+\theta-m+\theta<u-s$ 时, $p^{u-s-(n-u+r+\theta)+(m-\theta)}\mid l$. 由于

$$\theta+u-s-(n-u+r+\theta)+(m-\theta)=u-s-(n-u+r+\theta)+m<u-s,$$

因此 $\sigma'\equiv\sigma(\mathrm{mod}\ \min\{p^{u-s-(n-u+r+\theta)+m},p^{u-r}\})$.

类似子情形 1.2.1 的证明, 总可取适当的元素满足前面的定义关系且使得

$$\begin{cases}\sigma\leqslant\min\{p^\theta,p^{u-s}\}, & n-u+r+\theta-m+\theta\geqslant u-s,\\ \sigma\leqslant\min\{p^{u-s-(n-u+r+\theta)+m},p^{u-r}\}, & n-u+r+\theta-m+\theta<u-s.\end{cases}$$

综上可得定理中的群 (Ⅳ)

子情形 2.2 $\langle b,c\rangle$ 非交换.

类似定理 10.2.3 的证明, 可得 $s\leqslant t<\min\{u,n-u+r+\theta-m+\theta+s\}$.

子情形 2.2.1 $s=t$.

令 $a_1=ab^{-1}$. 则

$$a_1^{-1}ca_1=c,\quad a_1^{p^{n-u+r+\theta}}=c^{p^{r+\theta}(i-p^{n-u+r+\theta-m})}.$$

记 $[a_1,b]=c^{\sigma'}$. 接下来, 令 $a_2=a_1^k$, 其中

$$(i-p^{n-u+r+\theta-m})k\equiv 1(\mathrm{mod}\ p^{u-r-\theta}),\quad [a_2,b]=c^{k\sigma'}=c^\sigma.$$

不妨用 a 替换 a_2, 则有下面的定义关系:

$$a^{p^{n-u+r+\theta}}=c^{p^{r+\theta}},\quad b^{m-\theta}=c^{p^r},\quad c^{p^u}=1,\quad [a,b]=c^\sigma,\quad [c,a]=1,\quad [c,b]=c^{p^t},$$

其中

$$r+1\leqslant u\leqslant m\leqslant n,\quad r+\theta\leqslant u,\quad m-\theta+t\geqslant u,$$

$$r+t\geqslant u,\quad t<u,\quad r+\theta<m<n-u+r+\theta,\quad p\nmid\sigma,$$

且 σ 为一个正整数. 由定理 1.11.5 可知

$$[a,b^{p^{m-\theta}}]=[a,c^{p^r}]=1,\quad [a,b]^{p^{m-\theta}}=1.$$

从而 $c^{\sigma p^{m-\theta}}=1$. 进而 $m-\theta\geqslant u$. 故

$$r+1\leqslant u\leqslant m<n-u+r+\theta,\quad \theta\leqslant\min\{u-r,m-u\},\quad u-r\leqslant t<u,\quad p\nmid\sigma,$$

并且 σ 为一个正整数.

因为 $|G_3|=p^{u-t}$, 所以 t 为不变量. 从而只需考虑当 σ 取何值时, 对应的群两两互不同构. 为方便证明用 $G(\sigma)$ 记群 G. 设 $G(\sigma)\cong G(\sigma')$. 在群 $G(\sigma)$ 中, 令

$$a_1=a^{i_1}b^{j_1}c^{k_1},\quad b_1=a^{i_2}b^{j_2}c^{k_2},\quad c_1=c^v,$$

其中 $i_1,i_2,j_1,j_2,k_1,k_2,v$ 为适当的正整数且 $p\nmid i_1j_2v$ 使得 a_1 , b_1 生成 $G(\sigma)$, 且 $a_1,b_1,c_1^{\sigma'}=[a_1,b_1]$ 满足 $G(\sigma')$ 的定义关系. 显然 $p^{n-u+r+\theta-m+\theta}\mid i_2$. 记 $i_2=lp^{n-u+r+\theta-m+\theta}$, 经计算知

$$\begin{cases}i_1p^{r+\theta}+j_1p^{r+(n-u+r+\theta)-(m-\theta)}\equiv vp^{r+\theta}(\mathrm{mod}\ p^u),\\ lp^{r+\theta}+j_2p^r\equiv vp^r(\mathrm{mod}\ p^u),\\ \sigma\dfrac{[(1+p^t)^{j_2}-1]i_1}{p^t}(1+p^t)^{j_1}+\sigma\dfrac{[1-(1+p^t)^{j_1}]i_2}{p^t}(1+p^t)^{j_2}\\ \quad+k_2[1-(1+p^t)^{j_1}]+k_1[(1+p^t)^{j_2}-1]=v\sigma',\\ (1+p^t)^{j_1}\equiv 1(\mathrm{mod}\ p^u),\\ (1+p^t)^{j_2}\equiv 1+p^t(\mathrm{mod}\ p^u).\end{cases}$$

类似子情形 2.1 的证明, 可得 $\sigma'\equiv\sigma(\mathrm{mod}\ \min\{p^{u-r-\theta},p^{u-t}\})$.

类似子情形 1.2.1 的证明, 总可取适当的元素满足前面的定义关系且使得 $\sigma\leqslant\min\{p^{u-r-\theta},p^{u-t}\}$. 从而可得定理中的群 (Ⅴ).

子情形 2.2.2 $s<t$.

因为 $|G_3|=p^{u-s}$, 所以 s 为不变量. 类似定理 10.2.3 可知, t 为不变量. 因此 n,m,u,r,s,t,θ 为 G 的不变量. 显然 G 具有如下定义关系:

$$a^{p^{n-u+r+\theta}}=c^{ip^{r+\theta}},\quad b^{p^{m-\theta}}=c^{p^r},\quad c^{p^u}=1,\quad [a,b]=c^\sigma,$$
$$a^{-1}ca=c^{1+p^s},\quad b^{-1}cb=c^{1+p^t},$$

其中

$$r+1\leqslant u\leqslant m<n-u+r+\theta,\quad \theta\leqslant u-r,\quad \theta<m-r,$$

$$u-r-\theta\leqslant s<t,\quad u-r\leqslant t<\min\{u,n-u+r+\theta-m+\theta+s\},\quad p\nmid i\sigma,$$

且 i,σ 为正整数.

下面考虑当 i,σ 取何值时，对应的群两两互不同构. 为方便证明，记 G 为 $G(i,\sigma)$. 假设 $G(i,\sigma)\cong G(i',\sigma')$. 在群 $G(i,\sigma)$ 中，令

$$a_1=a^{i_1}b^{j_1}c^{k_1},\quad b_1=a^{i_2}b^{j_2}c^{k_2},\quad c_1=c^{v},$$

其中 $i_1,i_2,j_1,j_2,k_1,k_2,v$ 为适当的整数且 $p\nmid i_1j_2v$ 使得 a_1, b_1 生成 $G(i,\sigma)$, 并且 $a_1,b_1,c_1^{\sigma'}=[a_1,b_1]$ 满足 $G(i',\sigma')$ 的定义关系. 显然 $p^{n-u+r+\theta-m+\theta}\mid i_2$. 记 $i_2=lp^{n-u+r+\theta-m+\theta}$, 经计算知

$$\text{(a)}\begin{cases}i_1ip^{r+\theta}+j_1p^{r+(n-u+r+\theta)-(m-\theta)}\equiv i'vp^{r+\theta}(\text{mod }p^u),\\ ilp^{r+\theta}+j_2p^r+k_2p^{m-\theta}\equiv vp^r(\text{mod }p^u),\\ \sigma\dfrac{[(1+p^s)^{i_1}-1]}{p^s}\dfrac{[(1+p^t)^{j_2}-1]}{p^t}(1+p^t)^{j_1}-\sigma\dfrac{[(1+p^s)^{i_2}-1]}{p^s}\dfrac{[(1+p^t)^{j_1}-1]}{p^t}(1+p^t)^{j_2}\\ \quad -k_2[(1+p^s)^{i_1}(1+p^t)^{j_1}-1]+k_1[(1+p^s)^{i_2}(1+p^t)^{j_2}-1]=v\sigma',\\ (1+p^s)^{i_1}(1+p^t)^{j_1}\equiv 1+p^s(\text{mod }p^u),\\ (1+p^s)^{i_2}(1+p^t)^{j_2}\equiv 1+p^t(\text{mod }p^u).\end{cases}$$

注意到 $s<t$. 由 [247] 中的定理 6.2.3 可知，存在适当的 L 使得 $(1+p^t)\equiv(1+p^s)^{Lp^{t-s}}(\text{mod }p^u)$, 其中 $p\nmid L$. 因此

$$(1+p^s)^{i_1}(1+p^t)^{j_1}=(1+p^s)^{i_1+j_1Lp^{t-s}}\equiv 1+p^s(\text{mod }p^u).$$

故可设 $i_1=1-j_1Lp^{t-s}+Kp^{u-s}$. 注意到

$$i_2=lp^{n-u+r+\theta-m+\theta},\quad t<n-u+r+\theta-m+\theta+s.$$

由 [247] 中的定理 6.2.3 可知，总存在适当的 M 使得

$$(1+p^s)^{i_2}\equiv(1+p^t)^{lMp^{(n-u+r+\theta)-(m-\theta)+s-t}}(\text{mod }p^u),$$

其中 $p\nmid M$. 因此

$$(1+p^s)^{i_2}(1+p^t)^{j_2}\equiv(1+p^t)^{lMp^{(n-u+r+\theta)-(m-\theta)+s-t}+j_2}(\text{mod }p^u)\equiv(1+p^t)(\text{mod }p^u).$$

故可假设 $j_2=1-lMp^{(n-u+r+\theta)-(m-\theta)+s-t}+Np^{u-t}$.

类似子情形 2.1 的证明可得, $\sigma'p^r\equiv\sigma(i_1-li'p^{\theta})p^r(\text{mod }p^u)$ 且

$$i_1ip^{r+\theta}-lii'p^{r+\theta+\theta}+j_1p^{r+(n-u+r+\theta)-(m-\theta)}\equiv i'j_2p^{r+\theta}(\text{mod }p^u).$$

故 (a) 中的四个同余式等价于下面的式子:

$$\begin{cases}\sigma'p^r\equiv\sigma(i_1-li'p^{\theta})p^r(\text{mod }p^u),\\ i_1ip^{r+\theta}-lii'p^{r+\theta+\theta}+j_1p^{r+(n-u+r+\theta)-(m-\theta)}\equiv i'j_2p^{r+\theta}(\text{mod }p^u),\\ i_1=1-j_1Lp^{t-s}+Kp^{u-s},\\ j_2=1-lMp^{(n-u+r+\theta)-(m-\theta)+s-t}+Np^{u-t},\end{cases}$$

其中 $p \nmid LM$ 且 K, L, M, N 为整数. 进而

$$\text{(b)} \quad \begin{cases} \sigma' \equiv \sigma(1 - j_1 L p^{t-s} + K p^{u-s} - l i' p^{\theta}) (\mathrm{mod}\ p^{u-r}), \\ \quad (1 - j_1 L p^{t-s} + K p^{u-s} - l i' p^{\theta}) i + j_1 p^{(n-u+r+\theta)-m} \\ \equiv i'(1 - l M p^{(n-u+r+\theta)-(m-\theta)+s-t} + N p^{u-t}) (\mathrm{mod}\ p^{u-r-\theta}), \\ i_1 = 1 - j_1 L p^{t-s} + K p^{u-s}, \\ j_2 = 1 - l M p^{(n-u+r+\theta)-(m-\theta)+s-t} + N p^{u-t}. \end{cases}$$

从而, 若 $G(i,\sigma) \cong G(i',\sigma')$, 则

$$\text{(c)} \quad \begin{cases} \sigma' \equiv \sigma (\mathrm{mod}\ \min\{p^{t-s}, p^{\theta}\}), \\ i' \equiv i (\mathrm{mod}\ \min\{p^{t-s}, p^{\theta}, p^{(n-u+r+\theta)-m}, p^{(n-u+r+\theta)-(m-\theta)+s-t}, p^{u-t}, p^{u-r-\theta}\}). \end{cases}$$

反之, 当 (c) 成立时, $G(i,\sigma)$ 与 $G(i',\sigma')$ 也未必同构. 下面将利用 (c) 式, 来给出 $G(i,\sigma)$ 与 $G(i',\sigma')$ 同构的充分条件.

因为 $\sigma' \equiv \sigma (\mathrm{mod}\ \min\{p^{t-s}, p^{\theta}\})$, 可设 $\sigma' = \sigma + U \min\{p^{t-s}, p^{\theta}\}$. 由 (b) 可知, $U \cdot \min\{p^{t-s}, p^{\theta}\} \equiv \sigma(-j_1 L p^{t-s} + K p^{u-s} - l i' p^{\theta}) (\mathrm{mod}\ p^{u-r})$. 故

$$U \equiv \sigma(-j_1 L p^{t-s-\min\{t-s,\theta\}} + K p^{u-s-\min\{t-s,\theta\}} - l i' p^{\theta-\min\{t-s,\theta\}}) (\mathrm{mod}\ p^{u-r-\min\{t-s,\theta\}}).$$

显然, 总可选择适当的元素满足上面的定义关系: $\sigma \leqslant \min\{p^{t-s}, p^{\theta}\}$. 下面取 $U = 0$. 从而总设

$$-j_1 L p^{t-s-\min\{t-s,\theta\}} + K p^{u-s-\min\{t-s,\theta\}} - l i' p^{\theta-\min\{t-s,\theta\}} = \lambda p^{u-r-\min\{t-s,\theta\}}.$$

因此根据 (b) 式可得

$$i + j_1 p^{(n-u+r+\theta)-m} \equiv i'(1 - l M p^{(n-u+r+\theta)-(m-\theta)+s-t} + N p^{u-t}) (\mathrm{mod}\ p^{u-r-\theta}).$$

故

$$\begin{aligned} i' \equiv i(1 &+ i' i^{-1} l M p^{(n-u+r+\theta)-(m-\theta)+s-t} - i' i^{-1} N p^{u-t} \\ &+ j_1 i^{-1} p^{(n-u+r+\theta)-m}) (\mathrm{mod}\ p^{u-r-\theta}). \end{aligned} \tag{10.10}$$

因为 $(1+p^s)^{p^{(n-u+r+\theta)-(m-\theta)}} \equiv (1+p^t)^{M p^{(n-u+r+\theta)-(m-\theta)+s-t}} (\mathrm{mod}\ p^u)$ 且

$$(1+p^t) \equiv (1+p^s)^{L p^{t-s}} (\mathrm{mod}\ p^u),$$

故

$$(1+p^s)^{p^{(n-u+r+\theta)-(m-\theta)}} \equiv (1+p^s)^{L M p^{(n-u+r+\theta)-(m-\theta)}} (\mathrm{mod}\ p^u).$$

因此 $(1-LM)p^{(n-u+r+\theta)-(m-\theta)}\equiv 0(\bmod p^{u-s})$. 进而若

$$(n-u+r+\theta)-(m-\theta)+s<u,$$

则不妨设 $LM=1+\beta p^{u-s-(n-u+r+\theta)+(m-\theta)}$.

下面再分两种情形来讨论:

(i) $\theta\leqslant t-s$.

因为 $\theta\leqslant t-s$, 故 $-j_1Lp^{t-s-\theta}+Kp^{u-s-\theta}-li'=\lambda p^{u-r-\theta}$. 因此

$$l=-j_1i'^{-1}Lp^{t-s-\theta}+i'^{-1}Kp^{u-s-\theta}-\lambda i'^{-1}p^{u-r-\theta}.$$

从而对于 (10.10),

$$\begin{aligned}i'\equiv i[1&+i^{-1}j_1(1-LM)p^{(n-u+r+\theta)-m}+i^{-1}KMp^{(n-u+r+\theta)-m+u-t}\\&-i^{-1}\lambda Mp^{u-r-\theta+(n-u+r+\theta)-(m-\theta)+s-t}-i'i^{-1}Np^{u-t}](\bmod p^{u-r-\theta}).\end{aligned}$$

因为 $t<(n-u+r+\theta)-(m-\theta)+s$ 且 $n-u+r+\theta>m$, 所以

$$u-r-\theta+(n-u+r+\theta)-(m-\theta)+s-t>u-r-\theta,$$

$$(n-u+r+\theta)-m+u-t>u-t.$$

从而

$$\begin{aligned}i'\equiv i[1&+i^{-1}j_1(1-LM)p^{(n-u+r+\theta)-m}\\&+(i^{-1}KMp^{(n-u+r+\theta)-m}-i'i^{-1}N)p^{u-t}](\bmod p^{u-r-\theta}).\end{aligned}$$

若 $n-u+r+\theta-(m-\theta)+r\geqslant u$, 则 $(n-u+r+\theta)-m\geqslant u-r-\theta$. 因此

$$i'\equiv i(1-i'i^{-1}Np^{u-t})(\bmod p^{u-r-\theta}).$$

因此总可选取适当的元素满足定义关系且使得

$$\sigma\leqslant\min\{p^{t-s},p^{\theta}\},\quad i\leqslant\min\{p^{u-t},p^{u-r-\theta}\}.$$

假设 $n-u+r+\theta-(m-\theta)+r<u$. 若 $u-t\leqslant(n-u+r+\theta)-m$, 则

$$\begin{aligned}i'\equiv i[1&+(i^{-1}j_1(1-LM)p^{(n-u+r+\theta)-m-u+t}\\&+i^{-1}KMp^{(n-u+r+\theta)-m}-i'i^{-1}N)p^{u-t}](\bmod p^{u-r-\theta}).\end{aligned}$$

因此总可选取适当的元素满足定义关系且使得

$$\sigma\leqslant\min\{p^{t-s},p^{\theta}\},\quad i\leqslant\min\{p^{u-t},p^{u-r-\theta}\}.$$

若 $u-t>(n-u+r+\theta)-m$, 断言

$$(n-u+r+\theta)-(m-\theta)+s<u.$$

若否, 则 $u-t>u-s-\theta$. 故 $\theta>t-s$, 矛盾. 因此

$$LM=1+\beta p^{u-s-(n-u+r+\theta)+(m-\theta)}.$$

从而

$$i'\equiv i[1-i^{-1}j_1\beta p^{u-s-\theta}+(i^{-1}KMp^{(n-u+r+\theta)-m}-i'i^{-1}N)p^{u-t}](\bmod p^{u-r-\theta}).$$

因为 $\theta\leqslant t-s$, 故 $u-s-\theta\geqslant u-t$. 因此

$$i'\equiv i[1-(i^{-1}j_1\beta p^{t-s-\theta}+i^{-1}KMp^{(n-u+r+\theta)-m}-i'i^{-1}N)p^{u-t}](\bmod p^{u-r-\theta}).$$

故总可选取适当的元素满足定义关系且使得

$$\sigma\leqslant\min\{p^{t-s},p^{\theta}\},\quad i\leqslant\min\{p^{u-t},p^{u-r-\theta}\}.$$

(ii) $\theta>t-s$.

因为 $\theta>t-s$, 所以 $j_1=KL^{-1}p^{u-t}-lL^{-1}i'p^{\theta-t+s}-\lambda L^{-1}p^{u-r-t+s}$. 因此对于 (10.10),

$$\begin{aligned}i'\equiv i[&1+i'i^{-1}lL^{-1}(LM-1)p^{(n-u+r+\theta)-(m-\theta)+s-t}-i'i^{-1}Np^{u-t}\\&+i^{-1}KL^{-1}p^{(n-u+r+\theta)-m+u-t}-i^{-1}\lambda L^{-1}p^{u-r-t+s+(n-u+r+\theta)-m}](\bmod p^{u-r-\theta}).\end{aligned}$$

因为 $\theta>t-s$, 所以 $u-r-t+s>u-r-\theta$. 注意到 $n-u+r+\theta>m$, 因此

$$u-r-t+s+(n-u+r+\theta)-m>u-r-\theta.$$

从而

$$\begin{aligned}i'\equiv i[&1+i'i^{-1}lL^{-1}(LM-1)p^{(n-u+r+\theta)-(m-\theta)+s-t}\\&+(i^{-1}KL^{-1}p^{(n-u+r+\theta)-m}-i'i^{-1}N)p^{u-t}](\bmod p^{u-r-\theta}).\end{aligned}$$

类似情形 (i) 的证明, 总可选取适当的元素满足群的定义关系且使得

$$\sigma\leqslant\min\{p^{t-s},p^{\theta}\},\quad i\leqslant\min\{p^{u-t},p^{u-r-\theta}\}.$$

综上可得定理中的群 (VI).

最后, 易证 (IV)—(VI) 两两互不同构. 且对于 (I)—(VI), 利用循环扩张理论, 可证 $|G|=p^{n+m+r}$. 并且计算可知, G' 循环且 G 的型不变量为 (n,m,r). 细节略去. □

10.3 真子群的导群至多 p 阶的 p 群

张军强等在文献 [256] 给出了真子群的导群至多 p 阶的有限 p 群的刻画, 他们称这样的 p 群为 D_1 群. 更一般地, 若 p 群 G 的真子群的导群的阶都整除 p^i, 则称 G 为 D_i 群. 显然, $\mathcal{A}_2$ 群是 D_1 群. 本节的材料取自文献 [256].

由 D_1 群的定义不难得到下面的结论.

引理 10.3.1 若 G 是 D_1 群. 则

(i) 对 G 的任意极大子群 M 均有 $|M'| = 1$ 或 p, 且 $M' \leqslant G' \bigcap Z(G)$;

(ii) 若 $H \leqslant G$, 则 H 也是 D_1 群;

(iii) 若 $N \trianglelefteq G$, 则 G/N 也是 D_1 群.

引理 10.3.2 [265] 设 G 是 p 群, M_1 和 M_2 是 G 的两个不同的极大子群. 则 $|G'| \leqslant p|M_1'M_2'|$.

证明 因为 M_i' char $M_i \trianglelefteq G$, 故 $M_i' \trianglelefteq G$, $i = 1, 2$. 令 $\overline{G} = G/M_1'M_2'$. 则 $\overline{M}_1, \overline{M}_2 \lessdot \overline{G}$, 且 $\overline{M}_1$ 和 $\overline{M}_2$ 是交换群. 若 $\overline{G}$ 交换, 则 $|\overline{G}'| = 1$. 若 $\overline{G}$ 非交换, 则 $Z(\overline{G}) = \overline{M}_1 \bigcap \overline{M}_2$. 因为 $\overline{M}_1 \bigcap \overline{M}_2$ 是 $\overline{G}$ 的二极大子群, 由定理 1.7.6 可得 $p|\overline{G}'| = |\overline{G}/Z(\overline{G})| = p^2$. 于是 $|\overline{G}'| = p$. □

引理 10.3.3 若 G 是 D_1 群. 则

(i) $|G'| \leqslant p^3$;

(ii) 若 $|G'| \geqslant p^2$, 则 $d(G) \leqslant 3$.

证明 (i) 若 G 的极大子群唯一, 则 G 循环, 结果成立. 若 G 有两个极大子群 A 和 B, 由 G 是 D_1 群可知, $|A'| \leqslant p$ 和 $|B'| \leqslant p$. 因此 $|A'B'| \leqslant p^2$. 由引理 10.3.2 可得 $|G'| \leqslant p^3$.

(ii) 若 $|G'| \geqslant p^2$. 由定理 1.7.7 可知, G 不是内交换 p 群. 又 G 是 D_1 群, 故 G 有极大子群 A 满足 $|A'| = p$. 若对 G 的任意极大子群 B 都有 $B' \leqslant A'$, 则 G/A' 内交换或交换. 若 G/A' 交换, 则 $G' \leqslant A'$, 而 $|G'| \geqslant p^2$, 矛盾. 从而 G/A' 内交换. 又由定理 1.7.7 可知 $d(G/A') = 2$. 而 $A' \leqslant \Phi(G)$, 故 $d(G) = d(G/A') = 2$, 结论成立. 假设 G 有极大子群 B 使得 $B' \nleqslant A'$. 因为 G 是 D_1 群, 故 $|A'| = |B'| = p$ 且 $A' \bigcap B' = 1$. 选择 $a_1, a_2 \in A$ 和 $a_3, a_4 \in B$ 使得 $[a_1, a_2] \neq 1$ 和 $[a_3, a_4] \neq 1$. 则

$$A' = \langle [a_1, a_2] \rangle, \quad B' = \langle [a_3, a_4] \rangle \quad \text{且} \quad |\langle a_1, a_2, a_3, a_4 \rangle'| \geqslant p^2.$$

从而

$$G = \langle a_1, a_2, a_3, a_4 \rangle \quad \text{且} \quad d(G) \leqslant 4.$$

下面只需证 $d(G) \neq 4$. 若否, 则 $\langle a_1, a_2, a_k\rangle < G$, 其中 $k \in \{3,4\}$, 并有 $\langle a_3, a_4, a_s\rangle < G$, 其中 $s \in \{1,2\}$. 因为 G 是 D_1 群, 故

$$\langle a_1, a_2, a_k\rangle' = \langle [a_1, a_2]\rangle \quad 且 \quad \langle a_3, a_4, a_s\rangle' = \langle [a_3, a_4]\rangle.$$

因此 $[a_1, a_k]$, $[a_2, a_k] \in \langle [a_1, a_2]\rangle$, $k \in \{3,4\}$, 并且 $[a_s, a_3]$, $[a_s, a_4] \in \langle [a_3, a_4]\rangle$, $s \in \{1,2\}$. 所以 $[a_s, a_k] \in \langle [a_1, a_2]\rangle \bigcap \langle [a_3, a_4]\rangle$, 从而 $[a_s, a_k] = 1$, 其中 $s = 1, 2$; $k = 3, 4$. 然而在这种情况下, $\langle a_1, a_2a_3, a_4\rangle$ 是 G 的真子群且 $|\langle a_1, a_2a_3, a_4\rangle'| = p^2$, 矛盾. □

引理 10.3.4 设 G 是非交换 p 群. 若 $d(G) = 2$, 则对任意的 $H < G$ 均有 $H' < G'$.

证明 设 $R < G'$ 是 G' 中指数为 p 的 G 的正规子群. 则 $(G/R)'$ 的阶为 p 且 $d(G/R) = 2$. 由定理 1.7.7 可知, G/R 内交换. 设 H 是 G 的极大子群. 则 $H' \leqslant R < G'$. □

引理 10.3.5 设 G 是有限 p 群. 若下列情况之一成立.

(i) $|G'| \leqslant p$;

(ii) $d(G) = 2, |G'| = p^2$;

(iii) $d(G) = 2, c(G) = 3, G' \cong \mathrm{C}_p^3$, 其中 $p > 2$;

(iv) $d(G) = 3, c(G) = 2, G' \cong \mathrm{C}_p^3$ 或 C_p^2,

则 G 是 D_1 群.

证明 (i) 结论显然. 由引理 10.3.4 即得 (ii).

(iii) 设 $G = \langle a, b\rangle$. 因为 $c(G) = 3$, 故 $G_4 = 1$, $G_3 \leqslant Z(G)$. 从而对任意 $x \in G_3$ 和 $u \in G$, 有 $x^u = x$. 注意到 $[a, a] = [b, b] = 1$. 由命题 1.1.5 可知

$$G_3 = \langle [a, b, b], [a, b, a], [b, a, b], [b, a, a]\rangle \quad 且 \quad G' = \langle [a, b], G_3\rangle.$$

因为对任意的 $x, y \in G$, 有

$$[x^{-1}, y] = [y, x]^{x^{-1}} = ([x, y]^{-1})^{x^{-1}} \quad 且 \quad G_3 \leqslant Z(G),$$

所以

$$[b, a, a] = [[a, b]^{-1}, a] = ([[a, b], a]^{-1})^{[a,b]^{-1}} = [[a, b], a]^{-1} = [a, b, a]^{-1},$$

$$[b, a, b] = [[a, b]^{-1}, b] = ([[a, b], b]^{-1})^{[a,b]^{-1}} = [[a, b], b]^{-1} = [a, b, b]^{-1}.$$

于是得到

$$G_3 = \langle [a, b, b], [a, b, a]\rangle \quad 且 \quad G' = \langle [a, b], [a, b, b], [a, b, a]\rangle.$$

由 $G_3 \leqslant Z(G)$, 易得 G' 交换. 因此, 对任意的 $x \in G'$, 可设

$$x = [a,b]^i[a,b,b]^j[a,b,a]^k,$$

其中 i, j 和 k 为整数. 因为 $G_3 \leqslant Z(G)$, 所以对任意的 $g \in G$, 有

$$[x,g] = [[a,b]^i[a,b,b]^j[a,b,a]^k, g] = [[a,b]^i, g] = [[a,b],g]^i = [a,b,g]^i \in \langle [a,b,g] \rangle.$$

这说明 $[G', g] = \langle [a,b,g] \rangle$. 对任意的 $z, g \in G$ 和正整数 $n > 1$, 由命题 1.1.3(4) 可得

$$[z^n, g] = [z,g][z,g,z^{n-1}][z^{n-1}, g].$$

又由 $G_3 \leqslant Z(G)$ 和命题 1.1.7 可得

$$[z,g,z^{n-1}] = [z^{n-1},[z,g]]^{-1} = ([z,[z,g]]^{n-1})^{-1} = [z,g,z]^{n-1}.$$

从而有

$$[z^n, g] = [z,g][z^{n-1}, g][z,g,z]^{n-1}.$$

因此, 归纳易证

$$[z^n, g] = [z,g]^n [z,g,z]^{\frac{n(n-1)}{2}},$$

其中 $n > 1$. 取 $n = p$, 并且由 $G' \cong \mathrm{C}_p^3$ 和 $p > 2$ 得到

$$[z^p, g] = [z,g]^p [z,g,z]^{\frac{p(p-1)}{2}} = 1.$$

这说明

$$\mho_1(G) = \langle z^p \mid z \in G \rangle \leqslant Z(G).$$

又因为 $\Phi(G) = G'\mho_1(G)$, 所以 $[\Phi(G), g] = \langle [a,b,g] \rangle$. 于是对任意的 $x \in \Phi(G)$ 和 g, $h \in G$ 有

$$[x,g]^h = ([a,b,g]^i)^h = [a,b,g]^i.$$

令 M 是 G 的一个极大子群. 因为 $d(G) = 2$, 所以 $M/\Phi(G) = \langle \bar{g} \rangle$, 其中 $g \in G$, 于是 $M = \Phi(G)\langle g \rangle$. 又由命题 1.1.5 得

$$M' = \langle [x,g]^h \,|\, x \in \Phi(G), h \in M \rangle = \langle [a,b,g] \rangle.$$

从而 $|M'| \leqslant p$. 因此 G 是 D_1 群.

(iv) 因为 $c(G) = 2$ 且 $G' \cong \mathrm{C}_p^3$ 或 C_p^2, 故 $G' \leqslant Z(G)$ 且 $\exp(G') = p$. 从而对任意的 $x, y \in G$ 均有 $[x^p, y] = [x,y]^p = 1$. 故 $\mho_1(G) \leqslant Z(G)$. 于是 $\Phi(G) = G'\mho_1(G) \leqslant$

$Z(G)$. 因为 $d(G)=3$, 故 $G/\Phi(G)$ 是 p^3 阶初等交换 p 群, 并且 G 的任意极大子群可写为 $M=\langle\Phi(G),g_1,g_2\rangle=\Phi(G)\langle g_1,g_2\rangle$. 由命题 1.1.5 可知

$$M'=\langle [x,y]^h | x,y\in\Phi(G)\bigcup\{g_1,g_2\},h\in M\rangle=\langle [g_1,g_2]\rangle,$$

从而 $|M'|\leqslant p$. 因此 G 是 D_1 群. □

引理 10.3.6 若 G 是二元生成的 p 群, 则 $\Phi(G')G_3\lessdot G'$.

证明 因为 $d(G)=2$, 故 G'/G_3 循环. 由此可得 $G'/\Phi(G')G_3$ 循环. 又 $\exp(G'/\Phi(G')G_3)=p$, 故 $|G'/\Phi(G')G_3|=p$. 从而 $\Phi(G')G_3\lessdot G'$. □

引理 10.3.7 [265] 设 G 是 p 群, $N<G'$ 且 $N\lhd G$. 若 G/N 亚循环, 则 G 亚循环.

证明 令 $M\lessdot G'$, $N\leqslant M$ 且 $M\unlhd G$. 则 $|(G/M)'|=|G'/M|=p$. 由此可得 $\Phi((G/M)')=(G/M)_3=1$. 于是 $\Phi(G')G_3\leqslant M$. 由引理 10.3.6 可得 $M=\Phi(G')G_3$. 因为 G/N 亚循环且 $N\leqslant M$, 故 G/M 亚循环. 由定理 2.5.3 即得 G 亚循环. □

定理 10.3.8 设 G 是有限 p 群. 则 G 为 D_1 群当且仅当下列之一成立.

(i) $|G'|\leqslant p$;

(ii) $d(G)=2,|G'|=p^2$;

(iii) $d(G)=2,c(G)=3,G'\cong \mathrm{C}_p^3$, 其中 $p>2$;

(iv) $d(G)=3,c(G)=2,G'\cong \mathrm{C}_p^3$ 或 C_p^2.

证明 由引理 10.3.5 可知, 若 G 满足定理 10.3.8 中的条件 (i)—(iv) 之一, 则 G 是 D_1 群. 反之, 设 G 是 D_1 群. 只需证 G 为定理 10.3.8 的类型 (i)—(iv) 之一即可. 首先, 对 G 的任意极大子群 M, 由引理 10.3.1 可知, $|M'|=1$ 或 p, $M'\leqslant G'\bigcap Z(G)$. 又由引理 10.3.3 可得, $|G'|\leqslant p^3$, 且当 $|G'|\geqslant p^2$ 时 $d(G)\leqslant 3$. 不妨设 $|G'|\geqslant p^2$. 分下列两种情形完成证明.

情形 1 $|G'|=p^2$ 且 $d(G)\leqslant 3$.

由定理 1.7.7 可知, G 既非交换也非内交换. 因此 G 有极大子群 A 满足 $|A'|=p$. 若对 G 的任意极大子群 M 均有 $M'\leqslant A'$, 则 G/A' 的极大子群交换. 再由 $|G'/A'|=p>1$ 得 G/A' 非交换. 故 G/A' 内交换. 由 $A'\leqslant\Phi(G)$ 和定理 1.7.7 得 $d(G)=d(G/A')=2$. 此时 G 为定理 10.3.8 的类型 (ii). 若 G 有极大子群 B 满足 $B'\nleqslant A'$, 由 $A'\leqslant Z(G),B'\leqslant Z(G)$ 且 $|G'|=p^2$ 可得 $G'=A'B'\leqslant Z(G)$ 且 $G'\cong\mathrm{C}_p^2$. 若 $G=\langle a,b\rangle$, 由 $G'\leqslant Z(G)$ 得 $G'=\langle [a,b]\rangle$, 矛盾于 $G'\cong\mathrm{C}_p^2$. 若 $d(G)=3$, 由 $G'\leqslant Z(G)$ 得 $c(G)=2$, 此时 G 为定理 10.3.8 的类型 (iv).

情形 2 $|G'|=p^3$ 且 $d(G)\leqslant 3$.

由引理 10.3.2 知, G 有极大子群 A 和 B 满足 $|A'B'|=p^2$. 又由引理 10.3.1 得

$$A'B'\leqslant Z(G)\quad 且\quad A'B'=A'\times B'\cong\mathrm{C}_p^2.$$

由于 $G'/A'B'$ 循环且 $A'B' \leqslant Z(G)$, 故 G' 交换, 从而 G 亚交换. 于是 $G' = \mathrm{C}_{p^2} \times \mathrm{C}_p$ 或 $G' \cong \mathrm{C}_p^3$. 因为 $G' \neq A'B'$, 故 $G/A'B'$ 非交换.

假设对 G 的每个极大子群 M 均有 $M' \leqslant A'B'$. 则 $G/A'B'$ 的极大子群均交换. 故 $G/A'B'$ 内交换. 若 $G/A'B'$ 亚循环, 由引理 10.3.7 得 G 亚循环. 于是 G' 循环. 这矛盾于 $A'B' \cong \mathrm{C}_p^2$. 因此 $G/A'B'$ 非亚循环. 由定理 1.7.10, 不妨设

$$G/A'B' = \overline{G} = \langle \bar{a}, \bar{b} | \bar{a}^{p^n} = \bar{b}^{p^m} = \bar{c}^p = \bar{1}, [\bar{a}, \bar{b}] = \bar{c}, [\bar{c}, \bar{a}] = \bar{1}, [\bar{c}, \bar{b}] = \bar{1} \rangle,$$

其中, 若 $p = 2$, 则 $m + n \geqslant 3$. 易得 $\overline{G}_2 = \langle \bar{c} \rangle$ 且 $\overline{G}_3 = 1$. 因为 $A'B' \leqslant \Phi(G) \bigcap Z(G)$, 有 $G_3 \leqslant Z(G)$, 即 $G_4 = 1$. 令 a 和 b 分别是 $\bar{a}$ 和 $\bar{b}$ 在 G 中的原像, 并且 $[a, b] = d$. 那么 $G = \langle a, b, \Phi(G) \rangle = \langle a, b \rangle$, 并且 $\bar{d} = \bar{c}$. 设 $[d, a] = z_1$, $[d, b] = z_2$, 其中 $z_1, z_2 \in A'B'$. 由命题 1.1.5 得 $G' = \langle [a, b], G_3 \rangle$. 因为

$$[b, a, b] = z_2^{-1}, \quad [b, a, a] = z_1^{-1}, \quad G_4 = 1,$$

由引理 10.3.5(iii) 的证明可得

$$G_3 = \langle [a, b, b], [a, b, a], [b, a, b], [b, a, a] \rangle = \langle z_1, z_2 \rangle.$$

于是 $G' = \langle d, z_1, z_2 \rangle$. 若 $z_i \in \langle d \rangle$, $i = 1, 2$, 则 $G' = \langle d \rangle$, 矛盾于 $A' \times B' \leqslant G'$. 因此 z_1 或者 $z_2 \notin \langle d \rangle$. 不失一般性, 令 $z_2 \notin \langle d \rangle$. 因为 $G_3 \leqslant Z(G)$, 应用引理 10.3.5(iii) 的证明中同样的方法可得, $[a^p, b] = d^p z_1^{\frac{p(p-1)}{2}}$ 且 $[a, b^p] = d^p z_2^{\frac{p(p-1)}{2}}$.

若 $G' \cong \mathrm{C}_{p^2} \times \mathrm{C}_p$. 则 $A'B' = \langle d^p, z_2 \rangle$. 因为 $z_i \in A' \times B'$, 故 $|d| = p^2$. 由于 $\Phi(G) = G'\mho_1(G)$ 且 $d(G) = 2$, 于是对任意的 $x \in G$, $\langle x, G'\mho_1(G) \rangle$ 是 G 的真子群. 若 $p > 2$, 则 $z_1^{\frac{p(p-1)}{2}} = 1$ 且 $[a^p, b] = d^p$. 因为 a^p 和 d 都在 $G'\mho_1(G)$ 中, 故 $\langle b, G'\mho_1(G) \rangle' \geqslant \langle d^p, z_2 \rangle \cong \mathrm{C}_p^2$, 矛盾. 若 $p = 2$, 由 $z_1 \in A'B' = \langle d^2, z_2 \rangle$ 可得 $z_1 = 1$, d^2, z_2 或 $d^2 z_2$. 若 $z_1 = 1$, 则 $[a^2, b] = d^2$, 故 $\langle b, G'\mho_1(G) \rangle' \geqslant \langle d^2, z_2 \rangle \cong \mathrm{C}_2^2$. 若 $z_1 = d^2$ 或 z_2, 则 $[a, b^2] = d^2 z_2$. 由 $[d, a] = d^2$ 或 z_2, 有 $\langle a, G'\mho_1(G) \rangle' \geqslant \langle d^2, z_2 \rangle \cong \mathrm{C}_2^2$. 若 $z_1 = d^2 z_2$, 则

$$[a^2, ab] = [a^2, b] = d^2 z_1 = z_2 \quad 且 \quad [d, ab] = [d, a][d, b] = z_1 z_2 = d^2.$$

所以 $\langle ab, G'\mho_1(G) \rangle' \geqslant \langle d^2, z_2 \rangle \cong \mathrm{C}_2^2$. 综上所述, G 有一个真子群 M 满足 $M' \geqslant \langle d^2, z_2 \rangle \cong \mathrm{C}_2^2$, 这矛盾于 G 是 D_1 群.

若 $G' \cong \mathrm{C}_p^3$. 则 $d^p = 1$ 且 $G' = \langle d \rangle \times \langle z_1 \rangle \times \langle z_2 \rangle$. 若 $p = 2$, 因为 $\exp(G') = p$, 有 $[a, b^2] = [a, b, b] = z_2$, 然而 G 有极大子群 $\langle a^2, b^2, d, z_1, z_2, a \rangle$, 它的导群为 $\langle z_1, z_2 \rangle$. 这矛盾于 G 是 D_1 群. 若 $p > 2$, G 为定理 10.3.8 的类型 (iii).

设 G 有三个极大子群 A, B 和 C 满足 $|A'B'C'| = p^3$. 则

$$G' = A'B'C' = A' \times B' \times C' \leqslant Z(G).$$

从而 $G' \cong \mathrm{C}_p^3$. 若 $d(G) = 2$, 令 $G = \langle a, b\rangle$. 因为 $G' \leqslant Z(G)$, 由命题 1.1.5 得 $G' = \langle [a, b]\rangle$. 这矛盾于 $G' \cong \mathrm{C}_p^3$. 故 $d(G) \neq 2$. 若 $d(G) = 3$, 则 G 为定理 10.3.8 的类型 (iv). □

由定理 10.3.8, 容易给出 D_1 群的另一描述.

推论 10.3.9 设 G 是 p 群. 则 G 是非交换的 D_1 群当且仅当下列之一成立.

(i) $G = (A_1 * A_2 * \cdots * A_s)Z(G)$, 其中 $A_1, \cdots, A_s$ 为 G 的内交换子群;

(ii) G 亚循环且 $|G'| = p^2$;

(iii) $G' \bigcap Z(G)$ 中存在子群 N, 其中 $|N| = p$ 或 $N \cong \mathrm{C}_p^2$ 使得 G/N 为非亚循环的内交换 p 群;

(iv) $G' \bigcap Z(G)$ 中存在子群 N, 其中 $N \cong \mathrm{C}_p^3$ 或 C_p^2 使得 G/N 交换.

证明 只需证推论中描述的群满足定理 10.3.8 的条件之一即可. 对于群 (i), 显然 $|G'| = p$. 对于群 (ii), $G' \bigcap Z(G)$ 中存在 p 阶子群 N 使得 $d(G/N) = 2$ 且 $|(G/N)'| = p$. 由定理 1.7.7 可知, G/N 内交换. 再由定理 10.3.8 的证明可知, G 有下列两种可能的情形.

(1) G 亚循环且 $|G'| = p^2$,

或

(2) $G' \bigcap Z(G)$ 中存在 p 阶子群 N 使得 G/N 为非亚循环的内交换 p 群.

对于群 (iii), 由定理 10.3.8 的证明可知, $G' \bigcap Z(G)$ 中存在子群 N, 其中 $N \cong \mathrm{C}_p^2$ 使得 G/N 为非亚循环的内交换 p 群. 对于群 (iv), 因为 $c(G) = 2$, 故 $G' \bigcap Z(G)$ 中存在子群 N , 其中 $N \cong \mathrm{C}_p^3$ 或 C_p^2 使得 G/N 交换. 结论成立. □

10.4 非亚循环的真子群均为 D_1 群的 p 群

本节推广文献 [256] 的工作, 分类真子群亚循环或真子群的导群至多 p 阶的有限 p 群. 该分类由张丽华等在文献 [265] 中完成. 为方便, 这样的群简称为 $\mathcal{P}$ 群. 因为亚循环 p 群已被分类, 以下总假设 $\mathcal{P}$ 群是非亚循环的.

关于亚循环 p 群, 我们有下列简单结论, 在此不加证明地列于下面.

引理 10.4.1 设 G 是亚循环 p 群. 则下列结论成立.

(1) $d(G) \leqslant 2$ 且 G' 循环;

(2) $G' \leqslant \mho_1(G)$;

(3) 若 $H \leqslant G$, 则 H 亚循环;

(4) 若 $N \trianglelefteq G$, 则 G/N 亚循环.

引理 10.4.1 的一个直接推论如下.

推论 10.4.2 *若 p 群 G 至少有一个亚循环的极大子群, 则 $\Phi(G)$ 亚循环.*

引理 10.4.3 *设 G 是 p 群且 $|G'|=p^3$. 则 G' 交换.*

证明 若否, 则 $|Z(G')|=p$. 由 [241] 中的Ⅳ, 定理 5.12 可得 G' 循环. 矛盾.□

引理 10.4.4 *设 G 是 p 群且 $\exp(G')=p$. 则 $c(G)=2$ 当且仅当 $\Phi(G)\leqslant Z(G)$.*

证明 $\Longleftarrow$: 显然.

$\Longrightarrow$: 因为 $c(G)=2$, 故 $G'\leqslant Z(G)$. 又 $\exp(G')=p$, 故对任意的 $x,y\in G$ 均有 $[x^p,y]=[x,y]^p=1$. 由此可得 $\mho_1(G)\leqslant Z(G)$, 即 $\Phi(G)=G'\mho_1(G)\leqslant Z(G)$. □

引理 10.4.5 *设 G 是 p 群. 若 $G'\cong \mathrm{C}_p^3$. 则 $d(G)=2$ 当且仅当 $G/\Phi(G')G_3\cong \mathrm{M}_p(n,m,1)$.*

证明 $\Longleftarrow$: 因为 $d(G/\Phi(G')G_3)=2$ 且 $\Phi(G')G_3\leqslant\Phi(G)$, 故 $d(G)=2$.

$\Longrightarrow$: 因为 $d(G)=2$, 故 $d(G/\Phi(G')G_3)=2$. 另一方面, 由引理 10.3.6 可得

$$|(G/\Phi(G')G_3)'|=|G'/\Phi(G')G_3|=p.$$

于是由定理 1.7.7, 即得 $G/\Phi(G')G_3$ 内交换. 因为 G' 非亚循环, 由引理 10.4.1 可知 G 非亚循环. 再由定理 2.5.3 可得 $G/\Phi(G')G_3$ 非亚循环. 于是由定理 1.7.10 可得 $G/\Phi(G')G_3\cong \mathrm{M}_p(n,m,1)$. □

引理 10.4.6 *设 G 是 $\mathcal{P}$ 群. 则*

(1) 若 $H\leqslant G$, 则 H 是 $\mathcal{P}$ 群;

(2) 若 $N\trianglelefteq G$, 则 G/N 是 $\mathcal{P}$ 群.

证明 (1) 令 $K\lessdot H$. 则存在 $M\lessdot G$ 使得 $K\leqslant M$. 若 $|M'|\leqslant p$, 则 $|K'|\leqslant p$. 若 $|M'|>p$, 由 G 是 $\mathcal{P}$ 群可得 M 亚循环. 由引理 10.4.1(3) 得 K 亚循环. 故 H 是 $\mathcal{P}$ 群.

(2) 令 $M/N\lessdot G/N$. 则 $M\lessdot G$. 若 $|M'|\leqslant p$, 则 $|(M/N)'|\leqslant p$. 若 $|M'|>p$, 由 G 是 $\mathcal{P}$ 群可得 M 亚循环. 由引理 10.4.1(4), 即得 M/N 亚循环. □

引理 10.4.7 *设 G 是 $\mathcal{P}$ 群. 则*

(1) $G/\Omega_1(G')$ 所有真商群交换或亚循环;

(2) 若 G 至少有两个非亚循环的极大子群, 则 $|G'|\leqslant p^3$.

证明 (1) 令 $H/\Omega_1(G')<G/\Omega_1(G')$. 则 $H<G$. 若 $H/\Omega_1(G')$ 非亚循环, 则 H 非亚循环. 于是由引理 10.4.6 可得 $|H'|\leqslant p$. 因而 $H'\leqslant\Omega_1(G')$. 进一步地, $H/\Omega_1(G')$ 交换.

(2) 令 H 和 K 是 G 的两个不同的非亚循环的极大子群. 则 $|H'|\leqslant p$ 且 $|K'|\leqslant p$. 进一步地, $|H'K'|\leqslant p^2$. 由引理 10.3.2 推出 $|G'|\leqslant p^3$. □

有了以上的准备, 下面我们分类 $\mathcal{P}$ 群. 首先考虑恰有一个非亚循环的极大子群的 p 群.

定理 10.4.8 设 G 是恰有一个非亚循环的极大子群的 p 群, p 是奇素数. 则 G 是 $\mathcal{P}$ 群当且仅当 G 同构于下列不同构的群之一.

(1) $\mathrm{C}_{p^n} \times \mathrm{C}_p \times \mathrm{C}_p$, $n \geqslant 2$;

(2) $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^k}$, $k \geqslant 2$;

(3) $\mathrm{M}_p(n,1) \times \mathrm{C}_p$, $n \geqslant 2$;

(4) $\langle a,b,c \mid a^{p^n} = b^p = c^p = 1, [a,b] = c, [a,c] = [b,c] = 1\rangle \cong \mathrm{M}_p(n,1,1)$, $n \geqslant 2$;

(5) $\langle a,b,c \mid a^{p^{n+1}} = b^p = c^p = 1, [a,b] = c, [c,a] = a^{p^n}, [c,b] = 1\rangle$, $n \geqslant 2$;

(6) $\langle a,b,c \mid a^{p^{n+1}} = b^p = c^p = 1, [a,b] = c, [c,a] = 1, [c,b] = a^{vp^n}\rangle$, $n \geqslant 2, v = 1$ 或模 p 的平方非剩余.

证明 $\Longrightarrow$: 明显地, $|G| \geqslant p^4$ 且 $d(G) \leqslant 3$. 若 G 交换, 则 $d(G) = 3$. 此时, $G \cong \mathrm{C}_{p^n} \times \mathrm{C}_{p^m} \times \mathrm{C}_{p^k}$, 其中 $n \geqslant m \geqslant k$. 断言 $m = k = 1$. 若否, 则 $m \neq 1$. 于是存在 $M_1 \lessdot G$ 和 $M_2 \lessdot G$ 使得

$$M_1 \cong \mathrm{C}_{p^n} \times \mathrm{C}_{p^{m-1}} \times \mathrm{C}_{p^k} \quad 和 \quad M_2 \cong \mathrm{C}_{p^{n-1}} \times \mathrm{C}_{p^m} \times \mathrm{C}_{p^k}$$

是非亚循环的. 这与 G 恰有一个非亚循环的极大子群矛盾. 于是得到群 (1).

设 G 非交换. 令 $N \leqslant G'$ 满足 $|N| = p$ 且 $N \trianglelefteq G$, $\overline{G} = G/N$.

若 $\overline{G}$ 亚循环, 由 G 非亚循环及引理 10.3.7 可得 $G' = N$. 又 $d(\overline{G}) = d(G) = 2$, 由定理 1.7.7 可得 G 内交换. 又 G 非亚循环, 由定理 1.7.10 进一步可得 $G \cong \mathrm{M}_p(n,m,1)$. 断言 $m = 1$: 若否, 令 $M_1 = \langle a, b^p, c\rangle$ 且 $M_2 = \langle a^p, b, c\rangle$. 显而易见

$$M_1 \cong \mathrm{C}_{p^n} \times \mathrm{C}_{p^{m-1}} \times \mathrm{C}_p, \quad M_2 \cong \mathrm{C}_{p^{n-1}} \times \mathrm{C}_{p^m} \times \mathrm{C}_p.$$

因而 M_1 和 M_2 是 G 的两个不同的非亚循环的极大子群. 与假设矛盾. 于是得到群(4).

设 $\overline{G}$ 非亚循环. 则 $\overline{G}$ 内亚循环或 $\overline{G}$ 恰有一个非亚循环的极大子群.

若 $|G| = p^4$, 检查 p^4 阶群的分类可知, G 是群 (1), (3), 或 $n = 2$ 时的群 (4), 或 $k = 2$ 时的群 (2).

若 $|G| = p^5$, 检查由文献 [270] 给出的 p^5 阶群的分类可知, G 是定理中给出的群.

设 $|G| \geqslant p^6$. 则 $|\overline{G}| \geqslant p^5$. 由内亚循环 p 群的分类定理 8.1.1 可知, $\overline{G}$ 不是内亚循环群. 于是 $\overline{G}$ 恰有一个非亚循环的极大子群. 由归纳假设, $\overline{G}$ 同构于定理中的群之一.

情形 1 $\overline{G} \cong \mathrm{C}_{p^n} \times \mathrm{C}_p \times \mathrm{C}_p$.

此时, $d(G) = 3$ 且 $|G'| = p$. 满足这样条件的 p 群被 [8] 分类, 且已知 G 同构于 $\mathrm{M}_p(n,m,1) \times \mathrm{C}_{p^k}$, $\mathrm{M}_p(n,m,1) * \mathrm{C}_{p^{k+1}}$ 或 $\mathrm{M}_p(n+1,m) \times \mathrm{C}_{p^k}$ 之一.

若 $G\cong \mathrm{M}_p(n,m,1)\times \mathrm{C}_{p^k}$, 其中 $\mathrm{C}_{p^k}=\langle d\rangle$, 令 $M_1=\langle a,b,c^p\rangle$ 且 $M_2=\langle a^p,b,c,d\rangle$. 易见 $M_1\cong \mathrm{M}_p(n,m,1)\times \mathrm{C}_{p^{k-1}}$ 且 $M_2\cong \mathrm{C}_{p^{n-1}}\times \mathrm{C}_{p^m}\times \mathrm{C}_{p^k}\times \mathrm{C}_p$. 由此可知 M_1 和 M_2 是 G 的两个不同的非亚循环的极大子群. 与假设矛盾.

若 $G\cong \mathrm{M}_p(n,m,1)*\mathrm{C}_{p^{k+1}}$, 断言 $n=1$. 若否, 令 $M_1=\langle a,c^p,b\rangle$ 且 $M_2=\langle a^p,b,c\rangle$. 则 $M_1\cong \mathrm{M}_p(n,m,1)*\mathrm{C}_{p^k}$ 且 $M_2\cong \mathrm{C}_{p^{n-1}}\times \mathrm{C}_{p^m}\times \mathrm{C}_{p^k}$. 由此可知 M_1 和 M_2 是 G 的两个不同的非亚循环的极大子群. 与假设矛盾. 于是 $n=m=1$. 此为群(2).

若 $G\cong \mathrm{M}_p(n+1,m)\times \mathrm{C}_{p^k}$, 断言 $m=k=1$. 若否, 当 $k\neq 1$ 时, 令 $M_1=\langle a,c^p,b\rangle$ 且 $M_2=\langle a^p,b,c\rangle$. 则 $M_1\cong \mathrm{M}_p(n+1,m)\times \mathrm{C}_{p^{k-1}}$ 且 $M_2\cong \mathrm{C}_{p^n}\times \mathrm{C}_{p^m}\times \mathrm{C}_{p^k}$; 当 $m\neq 1$ 时, 令 $M_1=\langle a,b^p,c\rangle$ 且 $M_2=\langle a^p,b,c\rangle$. 则 $M_1\cong \mathrm{C}_{p^{n+1}}\times \mathrm{C}_{p^{m-1}}\times \mathrm{C}_{p^k}$ 且 $M_2\cong \mathrm{C}_{p^n}\times \mathrm{C}_{p^m}\times \mathrm{C}_{p^k}$. 在任何情形下, 我们看到, M_1 和 M_2 是 G 的两个不同的非亚循环的极大子群. 与假设矛盾. 于是 $m=k=1$. 此为群(3).

情形 2 $\overline{G}\cong \mathrm{M}_p(1,1,1)*\mathrm{C}_{p^k}$.

不妨设 $\overline{G}=\langle \bar{a},\bar{b},\bar{c}\mid \bar{a}^p=\bar{b}^p=\bar{c}^{p^k}=1,[\bar{a},\bar{b}]=\bar{c}^{p^{k-1}},[\bar{c},\bar{a}]=1,[\bar{c},\bar{b}]=1\rangle$. 因为 $|\overline{G}|>p^4$, 故 $k>2$. 令 $G=\langle a,b,c\rangle$. 注意到 $N\leqslant Z(G)$. 则 $[a,b,a]=[c^{p^{k-1}},a]=[c,a]^{p^{k-1}}=1$. 同理可得 $[a,b,b]=1$. 由此推出 $G_3=1$. 于是 $c(G)=2$. 因为 $b^p\in N\leqslant Z(G)$, 故 $[a,b]^p=[a,b^p]=1$. 因而 $G'=\langle [a,b],N\rangle\cong \mathrm{C}_p^2$ 且 $o(c)=p^k$. 令 $N=\langle d\rangle$. 则

$$G=\langle a,b,c\mid a^p=d^x,b^p=d^y,c^{p^k}=1,d^p=1,[a,b]=c^{p^{k-1}}d^i,[c,a]=d^j,[c,b]=d^t\rangle,$$

其中 x,y,i,j 和 t 是正整数, 且 $p\mid j$ 和 $p\mid t$ 至多一个成立. 易证 $\Phi(G)=\langle c^p,d\rangle$.

再分两种情形讨论: $x\equiv 0(\mathrm{mod}\ p)$ 或 $x\not\equiv 0(\mathrm{mod}\ p)$.

(i) $x\equiv 0(\mathrm{mod}\ p)$.

令 $M_1=\langle a,b,c^p,d\rangle$ 且 $M_2=\langle a,c,d\rangle$. 因为 M_1 和 M_2 均包含子群 $\langle a,c^{p^{k-1}},d\rangle\cong \mathrm{C}_p^3$, 故 M_1 和 M_2 是 G 的两个不同的非亚循环的极大子群. 与假设矛盾.

(ii) $x\not\equiv 0(\mathrm{mod}\ p)$.

若 $y\equiv 0(\mathrm{mod}\ p)$, 与(i)的论证相同, 可得 G 有两个不同的非亚循环的极大子群. 与假设矛盾. 若 $y\not\equiv 0(\mathrm{mod}\ p)$, 则 $b^p=a^{x^{-1}yp}$. 令 $b_1=ba^{-x^{-1}y}$. 则

$$b_1^p=1,\quad [a,b_1]=[a,b]=c^{p^{k-1}}d^i,\quad [c,b_1]=[c,a^{-x^{-1}y}][c,b]=d^{-x^{-1}yj}d^t=d^{t_1}.$$

这归结为 $y\equiv 0(\mathrm{mod}\ p)$ 的情形.

情形 3 $\overline{G}\cong \mathrm{M}_p(n,1)\times \mathrm{C}_p$.

类似于情形 2 的论证, 我们总能找到 G 的两个不同的非亚循环的极大子群. 这与假设矛盾. 因而这种情形不可能出现. 细节略去.

情形 4　$\overline{G} \cong \mathrm{M}_p(n,1,1)$.

不妨设 $\overline{G} = \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^n} = \bar{b}^p = \bar{c}^p = 1, [\bar{a},\bar{b}] = \bar{c}, [\bar{c},\bar{a}] = 1, [\bar{c},\bar{b}] = 1\rangle$. 令 $G = \langle a,b,c\rangle$. 因为 $|\overline{G}'| = p$, 故 $|G'| = p^2$. 于是 $|G_4| = 1$. 因而 $G_3 = \langle [a,b,a],[a,b,b]\rangle = \langle [c,a],[c,b]\rangle$. 注意到 $b^p \in N \leqslant Z(G)$. 于是

$$1 = [a,b^p] = [a,b]^p[a,b,b]^{\binom{p}{2}} = [a,b]^p[c,b]^{\binom{p}{2}} = [a,b]^p.$$

由此可得 $G' = \langle [a,b], N\rangle \cong \mathrm{C}_p^2$. 然而, 满足条件 $G' \cong \mathrm{C}_p^2$ 且 $G/N \cong \mathrm{M}_p(n,m,1)$ 的 p 群已被文献 [121] 分类及 G 是 [121] 中的定理 11 中的群 (1)—(7) 和 $m=1$ 时的群 (8). 从中挑出满足定理条件的群, 即得本定理中的群 (5) 和 (6).

情形 5　$\overline{G} = \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^n} = \bar{b}^p = \bar{c}^p = 1, [\bar{a},\bar{b}] = \bar{c}, [\bar{c},\bar{a}] = \bar{a}^{p^{n-1}}, [\bar{c},\bar{b}] = 1\rangle$.

令 $G = \langle a,b\rangle$. 因为 $|\overline{G}'| = p^2$, 故 $|G'| = p^3$. 由引理 10.4.3 推出 G' 交换. 于是 $G_4 = 1$ 且 $G_3 = \langle [c.a],[c,b]\rangle \neq 1$. 注意到 $b^p, c^p \in N \leqslant Z(G)$. 于是

$$1 = [a,b^p] = [a,b]^p[a,b,b]^{\binom{p}{2}} = [a,b]^p[c,b]^{\binom{p}{2}} = [a,b]^p,$$

$$1 = [a,c^p] = [a,c]^p[a,c,c]^{\binom{p}{2}} = [a,c]^p[a^{p^{n-1}},c]^{\binom{p}{2}} = [a,c]^p.$$

由此可得 $G' = \langle [a,b],[a,c],N\rangle \cong \mathrm{C}_p^3$, 且 $o(a)=p^n$, $o(c)=p$. 令 $N=\langle d\rangle$. 则 $[a,b]=c$, $[c,a] = a^{p^{n-1}}d^j$ 和 $[c,b] = d^t$, 其中 $t \not\equiv 0 \pmod p$.

若 $j \equiv 0 \pmod p$, 则

$$G = \langle a,b,c \mid a^{p^n} = 1, b^p = d^s, c^p = 1, d^p = 1, [a,b] = c, [c,a] = a^{p^{n-1}}, [c,b] = d^t\rangle,$$

其中 s 和 t 是正整数. 因为 $\Phi(G) = \langle a^p, c, d\rangle$, 令 $M_1 = \langle a^p, b, c, d\rangle$ 且 $M_2 = \langle a,c,d\rangle$. 验证易得 M_1 和 M_2 均包含子群 $\langle a^{p^{n-1}}, c, d\rangle \cong \mathrm{C}_p^3$. 因而 M_1 和 M_2 是 G 的两个不同的非亚循环的极大子群. 与假设矛盾.

若 $j \not\equiv 0 \pmod p$, 用 $ab^{-t^{-1}j}$ 替换 a 且令 $c = [ab^{-t^{-1}j}, b]$. 这归结为 $j \equiv 0 \pmod p$ 的情形.

情形 6　$\overline{G} = \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^n} = \bar{b}^p = \bar{c}^p = 1, [\bar{a},\bar{b}] = \bar{c}, [\bar{c},\bar{a}] = 1, [\bar{c},\bar{b}] = \bar{a}^{\nu p^{n-1}}\rangle$, 其中 $\nu = 1$ 或模 p 的平方非剩余.

令 $G = \langle a,b\rangle$. 因为 $|\overline{G}'| = p^2$, 故 $|G'| = p^3$. 由引理 10.4.3 可知 G' 交换. 于是 $G_4 = 1$ 且 $G_3 = \langle [c.a],[c,b]\rangle \neq 1$. 注意到 $b^p, c^p \in N \leqslant Z(G)$. 因而

$$1 = [a,b^p] = [a,b]^p[a,b,b]^{\binom{p}{2}} = [a,b]^p[c,b]^{\binom{p}{2}} = [a,b]^p,$$

$$1 = [b,c^p] = [b,c]^p[b,c,c]^{\binom{p}{2}} = [b,c]^p[a^{p^{n-1}},c]^{\binom{p}{2}} = [b,c]^p.$$

由此可得 $G'=\langle[a,b],[b,c],N\rangle\cong C_p^3$, $o(a)=p^n$ 且 $o(c)=p$. 令 $N=\langle d\rangle$. 则 $[a,b]=c$, $[c,a]=d^j$ 及 $[c,b]=a^{vp^{n-1}}d^t$. 于是

$$G=\langle a,b,c\mid a^{p^n}=1,b^p=d^s,c^p=1,d^p=1,[a,b]=c,[c,a]=d^j,[c,b]=a^{vp^{n-1}}d^t\rangle,$$

其中 s,j,t 是正整数且 $j\not\equiv 0(\mathrm{mod}\ p)$. 因为 $\Phi(G)=\langle a^p,c,d\rangle$, 令 $M_1=\langle a^p,b,c,d\rangle$ 且 $M_2=\langle a,c,d\rangle$. 验证易得 M_1 和 M_2 均包含子群 $\langle a^{p^{n-1}},c,d\rangle\cong C_p^3$. 因而 M_1 和 M_2 是 G 的两个不同的非亚循环的极大子群. 与假设矛盾.

我们还可证明定理中的互不同构且满足所设条件. 细节略去. 有兴趣的读者可看文献 [265]. □

恰有一个非亚循环的极大子群的 2 群已被 Janko 在文献 [99] 分类, 于是我们只需从中挑出 $\mathcal{P}$ 群即可. 定理 10.4.9 列出了结果, 而证明被略去.

定理 10.4.9 设 G 是恰有一个非亚循环的极大子群的 2 群. 则 G 是 $\mathcal{P}$ 群当且仅当 G 同构于下列互不同构的群之一.

(Ⅰ) $d(G)=3$.

(1) $C_{2^n}\times C_2\times C_2$, $n\geqslant 2$;

(2) $M_2(n,1)\times C_2$, $n\geqslant 3$;

(3) $Q_8 * C_{2^n}$, $n\geqslant 3$;

(4) $Q_8\times C_{2^n}$, $n\geqslant 2$;

(5) $\langle a,b,c\mid a^4=b^4=c^{2^n}=1,a^2=b^2,[a,c]=1,[c,b]=c^{2^{n-1}},[a,b]=a^2\rangle\cong Q_8 * C_{2^n}$, $n\geqslant 3$.

(Ⅱ) $d(G)=2$.

(6) $M_2(n,1,1)$, $n\geqslant 2$;

(7) $\langle a,b,c\mid a^{2^n}=b^2=c^2=1,[c,a]=b,[b,c]=1,[b,a]=a^{2^{n-1}}\rangle$, $n\geqslant 2$;

(8a) $\langle a,x\mid a^{2^m}\in\langle v\rangle,x^2\in\langle v^{2^{n-1}}\rangle,v^{2^n}=1,[a,x]=v,[v,x]\in\langle v^{2^{n-1}}\rangle,[v,a^2]=1,[a^2,x]=1,[v,a]=v^{-2}\rangle$, $m\geqslant 2$, $n\geqslant 2$;

(8b) $\langle a,x\mid a^{2^m}\in\langle v\rangle,x^2\in\langle v^{2^{n-1}}\rangle,v^{2^n}=1,[a,x]=v,[v,x]\in\langle v^{2^{n-1}}\rangle,[v,a^2]=1,[a^2,x]=v^{2^{n-1}},[v,a]=v^x,2^{n-1}|s+2\rangle$, $m\geqslant 2$, $n\geqslant 2$;

(8c) $\langle a,x\mid a^{2^m},x^2\in\langle v,b\rangle,v^2=b^2=[v,b]=1,[a,x]=v,[v,a]=b,[b,a]=[b,x]=1,[v,x]=z^t\in\langle v,b\rangle\bigcap Z(G),t=0,1\rangle$, $m\geqslant 2$;

(8d) $\langle a,x\mid a^{2^m}\in\langle v,b\rangle,x^2\in\langle v^2,b\rangle,v^4=b^2=1,[a,x]=v,[v,a]=b,[v,x]=v^2b,[b,a]=[b,x]=[v,b]=1\rangle$, $m\geqslant 2$;

(9) $\langle a,b,c\mid a^{2^2}=1,b^2,c^{2^m}\in\langle a^2\rangle,[a,b]=[a,c]=a^2,[c,b]=a\rangle$, $m\geqslant 2$;

(10) $\langle a,b\mid a^8=b^4=d^2=1,a^4=b^2=c,d^2=c^2=1,[a,b]=d,[d,a]=c,[d,c]=1\rangle$.

下面依照 p 群是否为 D_1 群来分类至少有两个非亚循环的极大子群, 且至少有一个亚循环的极大子群的 p 群. 如无特别说明, 所讨论的群总有这样的假设.

定理 10.4.10 设 G 不是 D_1 群. 则 G 是 $\mathcal{P}$ 群当且仅当 G 同构于下列互不同构的群之一.

(I) $c(G)=2$.

(1) $\langle a,b,c \mid a^{p^{n+2}}=b^{p^m}=c^p=1,[a,b]=a^{p^n},[a,c]=1,[b,c]=1\rangle$, $m\geqslant 2$.

(2) $\langle a,b,c \mid a^{p^{n+2}}=b^{p^m}=c^p=1,[a,b]=a^{p^n},[a,c]=a^{p^{n+1}},[b,c]=1\rangle$, $m\geqslant 3$, $n\geqslant 2$.

(3) $\langle a,b,c \mid a^{p^{n+2}}=b^{p^m}=c^p=1,[a,b]=a^{p^n},[a,c]=1,[b,c]=a^{p^{n+1}}\rangle$, $m\geqslant 2$, $n\geqslant 2$.

(4) $\langle a,b,c \mid a^{p^{n+2}}=b^{p^{m+1}}=c^p=1,[a,b]=a^{p^n},[a,c]=1,[b,c]=1,b^{p^m}=a^{p^{n+1}}\rangle$, $n+1<m$, $n\geqslant 2$.

(5) $\langle a,b,c \mid a^{p^{n+2}}=b^{p^{m+1}}=c^p=1,[a,b]=a^{p^n},[a,c]=a^{p^{n+1}},[b,c]=1,b^{p^m}=a^{p^{n+1}}\rangle$, $n+1\leqslant m$, $n\geqslant 2$.

(6) $\langle a,b,c \mid a^{p^{n+2}}=b^{p^{m+1}}=c^p=1,[a,b]=a^{p^n},[a,c]=1,[b,c]=a^{p^{n+1}},b^{p^m}=a^{p^{n+1}}\rangle$, $n+1<m$, $n\geqslant 2$.

(II) $c(G)=3$.

(7) $\langle a,b,c \mid a^{p^3}=b^{p^m}=c^p=1,[a,b]=a^p,[a,c]=1,[b,c]=1\rangle$, 若 $p>2$, 则 $m\geqslant 2$; 若 $p=2$, 则 $m\geqslant 1$.

(8) $\langle a,b,c \mid a^8=b^{2^m}=c^2=1,[a,b]=a^6,[a,c]=1,[b,c]=1\rangle$, $m\geqslant 1$.

(9) $\langle a,b,c \mid a^{p^3}=b^{p^m}=c^p=1,[a,b]=a^p,[a,c]=a^{p^2},[b,c]=1\rangle$, 若 $p>2$, 则 $m\geqslant 3$; 若 $p=2$, 则 $m\geqslant 1$.

(10) $\langle a,b,c \mid a^{p^3}=b^{p^m}=c^p=1,[a,b]=a^p,[a,c]=1,[b,c]=a^{p^2}\rangle$, 若 $p>2$, 则 $m\geqslant 2$; 若 $p=2$, 则 $m\geqslant 1$.

(11) $\langle a,b,c \mid a^{p^3}=b^{p^{m+1}}=c^p=1,[a,b]=a^p,[a,c]=1,[b,c]=1,b^{p^m}=a^{p^2}\rangle$, 若 $p>2$, 则 $m\geqslant 3$; 若 $p=2$, 则 $m\geqslant 2$.

(12) $\langle a,b,c \mid a^8=b^4=c^2=1,[a,b]=a^6,[a,c]=1,[b,c]=1,b^2=a^4\rangle$.

(13) $\langle a,b,c \mid a^{p^3}=b^{p^{m+1}}=c^p=1,[a,b]=a^p,[a,c]=a^{p^2},[b,c]=1,b^{p^m}=a^{p^2}\rangle$, 若 $p>2$, 则 $m\geqslant 3$; 若 $p=2$, 则 $m\geqslant 2$.

证明 设 M 是 G 的亚循环的极大子群. 于是 $d(G)\leqslant 3$. 由引理 10.4.7(2) 得 $|G'|\leqslant p^3$. 进一步断言 $|G'|\geqslant p^2$. 若否, 则 $|G'|\leqslant p$. 由定理 10.3.8 可知, G 是 D_1 群. 与假设矛盾. 故 $|G'|=p^2$ 或 p^3.

情形 1 $|G'|=p^3$.

由引理 10.4.3 可知 G' 交换. 令 M_1 和 M_2 是 G 的两个不同的非亚循环的极大子群. 由 $|G'|=p^3$ 和引理 10.3.2 推出 $|M_1'|=|M_2'|=p$ 且 $M_1'\bigcap M_2'=1$. 于是 $M_1'M_2'\cong \mathrm{C}_p^2$ 且 $M_1'M_2'\leqslant Z(G)$.

若 $G' \cong \mathrm{C}_{p^3}$, 则 G 有两个不同的 p 阶子群 M_1' 和 M_2', 矛盾. 若 $G' \cong \mathrm{C}_p^3$, 因为 G 是 $\mathcal{P}$ 群而不是 D_1 群, 故存在 $M \lessdot G$ 使得 $|M'| > p$ 且 M 亚循环. 由引理 10.4.1 推出 M' 循环. 然而由 $M' \leqslant G'$ 又得 $M' \cong \mathrm{C}_p^2$ 或 $M' \cong \mathrm{C}_p^3$, 矛盾.

下设 $G' \cong \mathrm{C}_{p^2} \times \mathrm{C}_p$. 因为 G 是 $\mathcal{P}$ 群而不是 D_1 群, 故存在 $M \lessdot G$ 使得 $|M'| > p$ 且 M 亚循环.

若 $d(G) = 2$, 令 $\overline{G} = G/M_1'M_2'$. 则 $\overline{G}$ 内交换. 于是 $M' = M_1'M_2' \cong \mathrm{C}_p \times \mathrm{C}_p$. 由引理 10.4.1 得 M' 循环. 矛盾. 设 $d(G) = 3$. 因为 G' 交换, 故 $|\Omega_1(G')| = |G'/\mho_1(G')| = |G'/\Phi(G')| = p^2$. 又 $M_1'M_2' \leqslant \Omega_1(G')$, 故 $\Omega_1(G') = M_1'M_2' \leqslant Z(G)$. 令 $\overline{G} = G/\Omega_1(G')$. 则 $d(\overline{G}) = 3$ 且 $|\overline{G}'| = p$. 于是 $\overline{G}$ 同构于 [8] 中的定理 3.1 中的群之一.

若 $\overline{G}$ 同构于 [8] 中的定理 3.1 中的群 (1), 即

$$\overline{G} \cong \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^4 = \bar{c}^{2^k} = 1,\ [\bar{a}, \bar{b}] = \bar{a}^2 = \bar{b}^2, [\bar{c}, \bar{a}] = 1, [\bar{c}, \bar{b}] = 1 \rangle,$$

此时 $G' = \langle [a, b] \rangle$ 且 $\Omega_1(G') \cong \mathrm{C}_4 \times \mathrm{C}_2$. 注意到 $\Omega_1(G') \cong \mathrm{C}_2^2$. 于是 $o([a, b]) = 4$. 因为 $[a, b] \equiv a^2 \equiv b^2 (\bmod\ \Omega_1(G'))$, 故 $1 = [a^2, b] = [a, b]^2[a, b, a] = [a, b]^2$. 矛盾.

若 $\overline{G}$ 同构于 [8] 中的定理 3.1 中的群 (2), 即

$$\overline{G} \cong \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^4 = \bar{c}^{2^{k+1}} = 1, [\bar{a}, \bar{b}] = \bar{a}^2 = \bar{b}^2 = \bar{c}^{2^k}, [\bar{c}, \bar{a}] = 1, [\bar{c}, \bar{b}] = 1 \rangle,$$

与上面相同的论证导出矛盾.

若 $\overline{G}$ 同构于 [8] 中的定理 3.1 中的群 (3), 即

$$\overline{G} \cong \langle \bar{a}, \bar{b}, \bar{c}, \bar{d} \mid \bar{a}^{p^n} = \bar{b}^{p^m} = \bar{c}^{p^k} = \bar{d}^p = 1, [\bar{a}, \bar{b}] = \bar{d}, [\bar{c}, \bar{a}] = 1, [\bar{c}, \bar{b}] = 1 \rangle,$$

此时 $\overline{G} \cong \mathrm{M}_p(n, m, 1) \times \mathrm{C}_{p^k}$, $\Phi(\overline{G}) = \langle \bar{a}^p, \bar{b}^p, \bar{c}^p, \bar{d} \rangle$. 于是 $\overline{M} = \langle \bar{a}, \bar{b}, \bar{c}^p, \bar{d} \rangle \lessdot \overline{G}$ 且 $|\overline{M}'| = p$. 若 $k > 1$, 则 $\overline{M} \cong \mathrm{M}_p(n, m, 1) \times \mathrm{C}_{p^{k-1}}$. 若 $k = 1$, 则 $\overline{M} \cong \mathrm{M}_p(n, m, 1)$. 然而由引理 10.4.7 可得 G 不是 $\mathcal{P}$ 群. 矛盾.

若 $\overline{G}$ 同构于 [8] 中的定理 3.1 中的群 (4), 即

$$\overline{G} \cong \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^n} = \bar{b}^{p^m} = \bar{c}^{p^{k+1}} = 1, [\bar{a}, \bar{b}] = \bar{c}^{p^k}, [\bar{c}, \bar{a}] = 1, [\bar{c}, \bar{b}] = 1 \rangle,$$

此时 $\overline{G} \cong \mathrm{M}_p(n, m, 1) * \mathrm{C}_{p^{k+1}}$. 由上面的论证可知, G 不是 $\mathcal{P}$ 群.

若 $\overline{G}$ 同构于 [8] 中的定理 3.1 中的群 (5), 即

$$\overline{G} \cong \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^{n+1}} = \bar{b}^{p^m} = \bar{c}^{p^k} = 1, [\bar{a}, \bar{b}] = \bar{a}^{p^n}, [\bar{c}, \bar{a}] = 1, [\bar{c}, \bar{b}] = 1 \rangle,$$

此时 $\overline{G} \cong \mathrm{M}_p(n+1, m) \times \mathrm{C}_{p^k}$, $\Phi(\overline{G}) = \langle \bar{a}^p, \bar{b}^p, \bar{c}^p \rangle$. 令 $G = \langle a, b, c \rangle$. 因为 $|\overline{G}'| = p$, 故 $G_4 = 1$. 于是

$$G_3 = \langle [a, b, b] \rangle, \quad G' = \langle [a, b], [c, a], [c, b], [a, b, b] \rangle.$$

注意到 $\Omega_1(G') \cong \mathrm{C}_p^2$. 于是 $o([a,b]) = p^2$, 且 $[a,c], [b,c]$ 和 $[a,b,a]$ 不同时属于 $\langle [a,b] \rangle$.

若 $[b,c] \notin \langle [a,b] \rangle$, 则存在 $M \lessdot G$ 使得 $\overline{M} = \langle \bar{a}^p, \bar{b}, \bar{c} \rangle \cong \mathrm{C}_{p^n} \times \mathrm{C}_{p^m} \times \mathrm{C}_{p^k}$. 于是 M 非亚循环. 计算可知 $o([a^p, b]) = p$ 且 $o([b,c]) = p$. 因为 $\langle [a^p, b] \rangle \neq \langle [b,c] \rangle$, 故 $|M'| > p$. 由此可得 G 不是 $\mathcal{P}$ 群. 若 $[a,c] \notin \langle [a,b] \rangle$ 或 $[a,b,a] \notin \langle [a,b] \rangle$, 类似于 $[b,c] \notin \langle [a,b] \rangle$ 的情形可证, G 不是 $\mathcal{P}$ 群.

综上所述, 不存在 $|G'| = p^3$ 的 $\mathcal{P}$ 群 G 使得 G 不是 D_1 群.

情形 2 $|G'| = p^2$.

若 $G' \cong \mathrm{C}_p^2$, 因为 G 是 $\mathcal{P}$ 群但不是 D_1 群, 故存在 $M \lessdot G$ 使得 $|M'| > p$ 且 M 亚循环. 故 M' 循环. 又 $M' \leqslant G'$, 故 $M' = G' \cong \mathrm{C}_p^2$. 矛盾. 因而 $G' \cong \mathrm{C}_{p^2}$.

因为 G 不是 D_1 群, 由定理 10.3.8 可得 $d(G) = 3$. 又 G' 交换, 故 $|\Omega_1(G')| = |G'/\mho_1(G')| = |G'/\Phi(G')| = p$. 于是 $\Omega_1(G') \leqslant Z(G)$. 令 $\overline{G} = G/\Omega_1(G')$. 则 $d(\overline{G}) = 3$ 且 $|\overline{G}'| = p$. 于是 $\overline{G}$ 同构于 [8] 中的定理 3.1 中的群之一.

若 $\overline{G}$ 同构于 [8] 中的定理 3.1 中的群 (1)—(4), 类似于情形 1 的论证可知, G 不是 $\mathcal{P}$ 群.

设 $\overline{G}$ 同构于 [8] 中的定理 3.1 中的群 (5), 即

$$\overline{G} \cong \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^{n+1}} = \bar{b}^{p^m} = \bar{c}^{p^k} = 1, [\bar{a}, \bar{b}] = \bar{a}^{p^n}, [\bar{c}, \bar{a}] = 1, [\bar{c}, \bar{b}] = 1 \rangle,$$

此时 $\overline{G} \cong \mathrm{M}_p(n+1, m) \times \mathrm{C}_{p^k}$ 且 $\Phi(\overline{G}) = \langle \bar{a}^p, \bar{b}^p, \bar{c}^p \rangle$. 于是 $\overline{M} = \langle \bar{a}, \bar{b}, \bar{c}^p \rangle \lessdot \overline{G}$ 且 $|\overline{M}'| = p$. 若 $k > 1$, 则 $\overline{M} \cong \mathrm{M}_p(n+1, m) \times \mathrm{C}_{p^{k-1}}$. 由引理 10.4.7 可得, G 不是 $\mathcal{P}$ 群. 矛盾. 下设 $k = 1$.

因为 $d(\overline{G}) = 3$, 故 $G = \langle a, b, c \rangle$. 又 $|\overline{G}'| = p$, 故 $G_4 = 1$. 于是

$$G_3 = \langle [a,b,b] \rangle = \langle [a,b]^{p^n} \rangle, \quad G' = \langle [a,b], [a,c], [b,c], [a,b,b] \rangle.$$

因为 $G' \cong \mathrm{C}_{p^2}$, 故 $[a,c]$ 和 $[b,c]$ 含在 $\Omega_1(G')$ 中. 因而 $G' = \langle [a,b] \rangle = \langle a^{p^n} \rangle$. 由此可得 $\Omega_1(G') = \langle a^{p^{n+1}} \rangle$. 若 $n \geqslant 2$, 则 $c(G) = 2$. 若 $n = 1$, 则 $c(G) = 3$. 以下分 $c(G) = 2$ 和 $c(G) = 3$ 两种情形讨论.

子情形 2.1 $c(G) = 2$.

显而易见 $o(a) = p^{n+2}$. 注意到 $\Omega_1(G') = \langle a^{p^{n+1}} \rangle$. 不妨设

$$[a,b] = a^{p^n}, \quad [a,c] = a^{ip^{n+1}}, \quad [b,c] = a^{jp^{n+1}}.$$

讨论 i 和 j 的可能取值.

(i) $i = j = 0$: 则

$$[a,b] = a^{p^n}, \quad [a,c] = 1, \quad [b,c] = 1. \tag{10.11}$$

(ii) $i \neq 0$ 且 $j = 0$: 令 $c_1 = c^{i^{-1}}$. 则

$$[a,b] = a^{p^n}, \quad [a,c] = a^{p^{n+1}}, \quad [b,c] = 1. \tag{10.12}$$

(iii) $j \neq 0$ 且 $i = 0$: 令 $c_1 = c^{j^{-1}}$. 则

$$[a,b] = a^{p^n}, \quad [a,c] = 1, \quad [b,c] = a^{p^{n+1}}. \tag{10.13}$$

(iv) $j \neq 0$ 且 $i \neq 0$:

若 $o(a) \geqslant o(b)$, 令 $a_1 = ab^t$, 其中 $t = -ij^{-1}$. 则 $[a_1, c] = 1$. 这归结为 (iii).

若 $o(a) < o(b)$, 令 $b_1 = ba^t$, 其中 $t = -ji^{-1}$. 则 $[b_1, c] = 1$. 这归结为 (ii).

再讨论 $o(b)$ 和 $o(c)$ 的取值.

首先断言 $o(b) \geqslant p^2$ 且 $o(c) = p$. 若否, 则 $o(b) = p$. 于是 $[a,b]^p = [a, b^p] = 1$, 矛盾. 若 $o(c) = p^2$, 则 $c^p = a^{tp^{n+1}}$. 令 $c_1 = ca^{-tp^n}$. 则 $c_1^p = (ca^{-tp^n})^p = 1$ 且满足 c 的关系式. 于是 $o(c) = p^2$ 可归结为 $o(c) = p$ 的情形. 因而仅需讨论 $o(b)$ 的值.

若 $o(b) = p^m$, 则 $m \geqslant 2$.

若 a, b 和 c 具有关系式 (10.11), 则

$$G = \langle a, b, c \mid a^{p^{n+2}} = b^{p^m} = c^p = 1, [a,b] = a^{p^n}, [a,c] = 1, [b,c] = 1 \rangle,$$

其中 $m \geqslant 2$ 且 $n \geqslant 2$. 此为群 (1).

若 a, b 和 c 具有关系式 (10.12), 则

$$G = \langle a, b, c \mid a^{p^{n+2}} = b^{p^m} = c^p = 1, [a,b] = a^{p^n}, [a,c] = a^{p^{n+1}}, [b,c] = 1 \rangle,$$

其中 $n \geqslant 2$. 若 $m = 2$, 令 $c_1 = cb^{-p}$. 则 $[a, c_1] = 1$. 这又得到群 (1). 若 $m \geqslant 3$, 此为群 (2).

若 a, b 和 c 具有关系式 (10.13), 则

$$G = \langle a, b, c \mid a^{p^{n+2}} = b^{p^m} = c^p = 1, [a,b] = a^{p^n}, [a,c] = 1, [b,c] = a^{p^{n+1}} \rangle,$$

其中 $m \geqslant 2$ 且 $n \geqslant 2$. 此为群 (3).

若 $o(b) = p^{m+1}$, 则 $m \geqslant 1$. 不妨设 $b^{p^m} = a^{sp^{n+1}}$, 其中 $(p, s) = 1$.

若 a, b 和 c 具有关系式 (10.11), 当 $n + 1 \geqslant m$ 时, 令 $b_1 = ba^{-sp^{n+1-m}}$, 则 $b_1^{p^m} = 1$. 这归结为 $o(b) = p^m$ 的情形. 若 $n + 1 < m$, 则

$$G = \langle a, b, c \mid a^{p^{n+2}} = b^{p^{m+1}} = c^p = 1, [a,b] = a^{p^n}, [a,c] = 1, [b,c] = 1, b^{p^m} = a^{p^{n+1}} \rangle.$$

此为群 (4).

若 a, b 和 c 具有关系式 (10.12), 当 $n+1>m$ 时, 令 $b_1 = ba^{-sp^{n+1-m}}$, 则 $b_1^{p^m}=1$. 这归结为 $o(b)=p^m$ 的情形. 若 $n+1\leqslant m$, 则

$$G=\langle a,b,c \mid a^{p^{n+2}}=b^{p^{m+1}}=c^p=1,[a,b]=a^{p^n},[a,c]=a^{p^{n+1}},[b,c]=1,b^{p^m}=a^{p^{n+1}}\rangle.$$

此为群 (5).

若 a, b 和 c 具有关系式 (10.13), 当 $n+1\geqslant m$ 时, 令 $b_1 = ba^{-sp^{n+1-m}}$, 则 $b_1^{p^m}=1$. 这归结为 $o(b)=p^m$ 的情形. 若 $n+1<m$, 则

$$G=\langle a,b,c \mid a^{p^{n+2}}=b^{p^{m+1}}=c^p=1,[a,b]=a^{p^n},[a,c]=1,[b,c]=a^{p^{n+1}},b^{p^m}=a^{p^{n+1}}\rangle.$$

此为群 (6).

子情形 2.2　$c(G)=3$.

此时 $o(a)=p^3$. 首先断言: 当 $p>2$ 时, 则 $o(b)\geqslant p^2$. 若否, 则 $o(b)=p$. 于是

$$1=[a,b^p]=[a,b]^p[a,b,b]^{\binom{p}{2}}=[a,b]^p.$$

矛盾. 注意到 $\Omega_1(G')=\langle a^{p^2}\rangle$. 不妨设

$$[a,b]=a^p,\quad [a,c]=a^{ip^2}\quad 且\quad [b,c]=a^{jp^2}\quad 若\quad p>2.$$

若 $p=2$, 则 $[a,b]=a^2$ 或 a^6. 不妨设 $[a,c]=a^{i2^2}$, $[b,c]=a^{j2^2}$. 与子情形 2.1 的论证方法类似, 讨论 i 和 j 的可能取值及 $o(b)$ 和 $o(c)$ 的可能取值即得定理中的群 (7)—(13).

反之可证, 定理中的群互不同构且满足假设条件. 证明细节可参看文献 [265]. □

由 D_1 群的结构刻画不难得到下述的 $\mathcal{P}$ 群的分类.

定理 10.4.11　*设 G 是 D_1 群. 则 G 是 $\mathcal{P}$ 群当且仅当 G 同构于下列群之一.*

(1) $\mathrm{C}_{p^n}\times\mathrm{C}_{p^m}\times\mathrm{C}_p$, $n\geqslant m>1$;

(2) $\langle a,b,c \mid a^{p^n}=b^p=c^{p^{k+1}}=1,[a,b]=c^{p^k},[c,a]=[c,b]=1\rangle\cong \mathrm{M}_p(n,1,1)*\mathrm{C}_{p^{k+1}}$, $n>1$;

(3) $\langle a,b,c \mid a^{p^n}=b^p=c^{p^k}=1,[a,b]=a^{p^{n-1}},[c,a]=[c,b]=1\rangle\cong \mathrm{M}_p(n,1)\times\mathrm{C}_{p^k}$, $n>1, k>1$;

(4) $\langle a,b,c \mid a^{p^n}=b^{p^m}=c^p=1,[a,b]=a^{p^{n-1}},[c,a]=[c,b]=1\rangle\cong \mathrm{M}_p(n,m)\times\mathrm{C}_p$, $n>1, m>1$;

(5) $\langle a,b,c \mid a^p=b^{p^{m+1}}=c^{p^{m+1}}=1,[b,c]=1,[c,a]=c^{p^m},[a,b]=b^{-p^m}\rangle$, $p>2$;

(6) $\langle a,b,c \mid a^p=b^{p^{m+1}}=c^{p^{m+1}}=1,[b,c]=1,[c,a]=b^{p^m}c^{p^m},[a,b]=b^{-p^m}\rangle$, $p>2$;

(7) $\langle a,b,c \mid a^p=b^{p^{m+1}}=c^{p^{m+1}}=1,[b,c]=1,[c,a]=b^{p^m}c^{tp^m},[a,b]=b^{-tp^m}c^{\nu p^m}\rangle$, $p>2$, $\nu=1$ 或是模 p 的平方非剩余, $t^2\neq-\nu$, $t\in\left\{0,1,\cdots,\dfrac{p-1}{2}\right\}$;

(8) $\langle a,b,c \mid a^2=b^{2^{m+1}}=c^{2^{m+1}}=1,[b,c]=1,[c,a]=b^{2^m},[a,b]=c^{2^m}\rangle$;

(9) $\langle a,b,c \mid a^2=b^{2^{m+1}}=c^{2^{m+1}}=1,[b,c]=1,[c,a]=c^{2^m},[a,b]=b^{2^m}\rangle$;

(10) $\langle a,b,c \mid a^2=b^{2^{m+1}}=c^{2^{m+1}}=1,[b,c]=1,[c,a]=b^{2^m},[a,b]=b^{2^m}c^{2^m}\rangle$;

(11) $\langle a,b,c \mid a^p=b^{p^{m+1}}=c^{p^{n+1}}=1,[b,c]=1,[a,b]=b^{p^m},[c,a]=c^{tp^n}\rangle$, $m>n$, $1\leqslant t\leqslant p-1$;

(12) $\langle a,b,c \mid a^p=b^{p^{m+1}}=c^{p^{n+1}}=1,[b,c]=1,[a,b]=c^{\nu p^n},[c,a]=b^{p^m}\rangle$, $m>n$, $\nu=1$ 或是模 p 的平方非剩余;

(13) $\langle a,b,c \mid a^{p^{l+1}}=b^p=c^{p^{n+1}}=1,[b,c]=1,[c,a]=c^{p^n},[a,b]=a^{p^l}\rangle$;

(14) $\langle a,b,c \mid a^{p^{l+1}}=b^{p^{m+1}}=c^p=1,[b,c]=1,[c,a]=b^{p^m},[a,b]=a^{p^l}\rangle$;

(15) $\langle a,b,c \mid b^4=c^4=1,a^2=b^2,[a,b]=c^2,[a,c]=b^2,[b,c]=1\rangle$.

定理 10.4.8— 定理 10.4.10、定理 10.4.11 分别给出了恰有一个非亚循环的极大子群的 $\mathcal{P}$ 群及至少有两个非亚循环的极大子群且至少有一个亚循环的极大子群的 $\mathcal{P}$ 群的分类. 对于极大子群均非亚循环的 $\mathcal{P}$ 群, 文献 [265] 也给出了分类. 从而 $\mathcal{P}$ 群被完全分类.

10.5 两个非交换元生成 p^3 阶子群的 p 群

我们知道, 最小阶的非交换 p 群是 p^3 阶的. 一个自然的问题是: 若对于非交换 p 群 G 的任意两个元 $x,y\in G$, 只要 $[x,y]\neq1$, 就有 $|\langle x,y\rangle|=p^3$, 这样的 p 群是什么样的? 更特殊的问题是: 若对于非交换 p 群 G 的任意两个元 $x,y\in G$ 都有 $|\langle x,y\rangle|\leqslant p^3$, 这样的 p 群又是什么样呢? 张勤海等在文献 [274] 中回答了这样的问题, 确定了这些群的结构. 为方便, 有限非交换 p 群 G 称为 $\mathcal{T}_i$ 群, 若 G 的任意两个非交换元生成 p^i 阶的内交换子群. 本节分类 $\mathcal{T}_3$ 群. 下节分类 $\mathcal{T}_4$ 群.

引理 10.5.1 [69] 设 G 是 p 群, $|G'|=p$ 且 G/G' 是初等交换的. 则 $G=E*A$, 其中 E 是超特殊 p 群, A 是交换群. 若 A 不初等交换, 则 $E\bigcap A=Z(E)=\mho_1(A)$.

命题 10.5.2 设 G 是 $\mathcal{T}_3$ 群. 则

(1) $c(G)\leqslant3$, 进一步地, 若 $p\neq3$, 则 $c(G)=2$;

(2) $\exp(G)\leqslant p^2$;

(3) 对任意的 $a\in G$, 其中 $o(a)=p^2$, 则 $\langle a\rangle\lhd G$, 特别地, $a^p\in Z(G)$;

(4) 若 $o(a)=p^2$ 且 $a\notin Z(G)$, 则 $C_G(\langle a\rangle)$ 是 G 的极大子群.

证明 (1) 对任意的 $a,b\in G$, 若 $[a,b]\neq1$, 则 $[a,b,b]=1$. 因为 $|\langle x,y\rangle|\leqslant p^3$, 故 G 满足 2-Engel 条件. 由 [89] 中的III, 定理 6.5, 结论即推出.

(2) 因为 G 非交换, 所以 G 有一个最高阶元 a 使得 $a \in G \backslash Z(G)$. 若否, 取一个非中心的元 b, 则 $ab \notin Z(G)$ 且 ab 有最高阶. 令 $b \in G$ 满足 $[a,b] \neq 1$. 设 $o(a) \geqslant p^3$. 则 $|\langle a,b\rangle| \geqslant p^4$. 矛盾.

(3) 对任意的 $b \in G$, 若 $[a,b]=1$, 则 b 正规化 a. 若 $[a,b] \neq 1$, 因为 $\langle a,b\rangle$ 是 p^3 非交换群, 故 b 也正规化 a. 于是 $\langle a\rangle \lhd G$.

(4) 由 N/C 定理得, $N_G(\langle a\rangle)/C_G(\langle a\rangle) = G/C_G(\langle a\rangle) \lesssim \mathrm{Aut}(\langle a\rangle)$. 则 p 恰整除 $|\mathrm{Aut}(\langle a\rangle)| = p(p-1)$. 结论由此推出. □

以下依照 $\exp(G)=p$ 与 $\exp(G)=p^2$ 两种情况分类 $\mathcal{T}_3$ 群.

定理 10.5.3 设 $\exp(G)=p$. 则 G 是 $\mathcal{T}_3$ 群当且仅当下列之一成立.

(1) $p=3$ 且 $c(G) \leqslant 3$;

(2) $p>3$ 且 $c(G)=2$.

证明 若 $p=2$, 则 $\exp(G)=2$ 隐含着 G 交换. 矛盾. 故 $p>2$. 由命题 10.5.2 可知, 若 G 是 $\mathcal{T}_3$ 群, 则 (1) 或 (2) 成立. 反之, 若 (1) 或 (2) 成立, 我们将证明 G 是 $\mathcal{T}_3$ 群. 设 (2) 成立. 因为 $c(G)=2$ 且 $\exp(G)=p$, 结论是明显的. 设 (1) 成立. 取 $a,b \in G$ 满足 $[a,b] \neq 1$. 令 $H=\langle a,b\rangle$. 因为 $\exp(G)=p$, 所以 G 是正则的. 由定理 4.2.12 知, H' 是循环的. 这隐含着 $|H'|=3$, 因而 $|H|=3^3$. 即得所求结论. □

以下我们假设 $\exp(G)=p^2$.

引理 10.5.4 p 群 G 是 $\mathcal{T}_3$ 群当且仅当 $G \times \mathrm{C}_p^n$ 是 $\mathcal{T}_3$ 群.

证明 只需证充分性. 令 $H = G \times \mathrm{C}_p^n$. 则 H 中任意两个非交换元 x 和 y 具有形式: $x=ac_1, y=bc_2$, 其中 $a,b \in G$, $c_1,c_2 \in \mathrm{C}_p^n$. 因为 $c_1,c_2 \in Z(H)$, 故 $[a,b] \neq 1$ 且 $|\langle a,b\rangle| \leqslant p^3$, 由此易得 $|\langle x,y\rangle| \leqslant p^3$. □

由此引理, 只需确定没有初等交换直因子的 $\mathcal{T}_3$ 群. 这样的 $\mathcal{T}_3$ 群称为基本的 $\mathcal{T}_3$ 群. 为方便起见，再引入一个概念: 设 A 是交换群满足 $\exp(A)>2$. 令 $\alpha: a \longmapsto a^{-1}, \forall a \in A$ 是 A 的自同构. 则半直积 $A \rtimes \langle\alpha\rangle$ 称为具有核 A 的广义二面体群.

定理 10.5.5 设 $\exp(G)=p^2$. 则 G 是基本的 $\mathcal{T}_3$ 群当且仅当下列之一成立.

(1) $p=2: G$ 是具有核 $\mathrm{C}_4^s (s \geqslant 1)$ 的广义二面体群, 或超特殊 p 群 E, 或 $E * \mathrm{C}_4$;

(2) $p \geqslant 3: G$ 是指数为 p^2 的超特殊 p 群 E, 或 $E * \mathrm{C}_{p^2}$.

证明 设 $p=2$. 依照两种情况讨论:

情形 1 对 G 的任意两个非交换元 x,y 都有 $\langle x,y\rangle \cong \mathrm{D}_8$.

由假设, 取 G 的子群 $\langle a,b \mid a^4=b^2=1, a^b=a^{-1}\rangle \cong \mathrm{D}_8$. 再由命题 10.5.2(4) 知, $C_G(a)$ 是 G 的极大子群, 因而 $G = C_G(a) \rtimes \langle b\rangle$.

首先我们断言: $C_G(a)$ 交换且 $\exp(Z(G))=2$.

设 $\exp(Z(G))=2$, $C_G(a)$ 不交换. 则它有子群 $\langle c,d\rangle \cong \mathrm{D}_8$ 且 $o(c)=4, o(d)=2$. 于是 $o(ad)=4$ 且 $[ad,c] \neq 1$. 因为 D_8 只有一个 4 阶子群, 故 $\langle ad,c\rangle \ncong \mathrm{D}_8$. 矛盾.

设 $\exp(Z(G)) > 2$. 令 $g \in Z(G)$ 且 $o(g) = 4$. 则 $[a, gb] \neq 1$, 因而 $\langle a, gb\rangle \cong \mathrm{D}_8$. 但 $\langle a, gb\rangle$ 的 4 阶子群不是一个. 矛盾.

其次, 因为 $C_G(a)$ 交换且 $\exp(G) = 2^2$, 可设 $C_G(a) = H \times K$, 其中

$$H = \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_s\rangle, \quad K = \langle c_1\rangle \times \langle c_2\rangle \times \cdots \times \langle c_t\rangle,$$

$o(a_i) = 4$, $o(c_j) = 2$, $i \geqslant 1$, $j \geqslant 0$. 断言: 对任意的 c_j 都有 $[b, c_j] = 1$. 否则, $\langle b, c_j\rangle \cong \mathrm{D}_8$. 令 $c_j = hb$. 则 $o(h) = 4$ 且 $[h, b] = h^2$. 另一方面, $1 = [c_j, a] = [hb, a] = [h, a]^b[b, a]$ 隐含着 $[h, a] \neq 1$. 由此可得 $\langle h, a\rangle \ncong \mathrm{D}_8$. 矛盾. 于是 $K \leqslant Z(G)$ 且 $G = (H \rtimes \langle b\rangle) \times K$. 因为 G 是基本的 $\mathcal{T}_3$ 群, 故 $K = 1$ 且 $G = H \rtimes \langle b\rangle$.

考虑 b 在 H 上的作用. 设 $h \in H$ 且 $o(h) = 4$. 因为 $\exp(Z(G)) = 2$, 故 $h \notin Z(G)$ 且 $h^b \neq h$. 又 $\langle h\rangle \lhd G$ 且 $o(b) = 2$, 有 $h^b = h^{-1}$. 由此可得 G 是具有核 H 的广义二面体群.

反之, 上述确定的群是 $\mathcal{T}_3$ 群. 事实上, 令 $x, y \in G$ 且 $[x, y] \neq 1$. 则 x 和 y 中的一个, 比如, y 不在 H 中, 则 $o(y) = 2$. 若 $x \in H$, 则 $\langle x, y\rangle \cong \mathrm{D}_8$. 若 $x \notin H$, 则 $xy \in H$ 且 $o(xy) = 4$. 这是因为若 $o(xy) = 2$, 则 $xy \in C_G(y)$. 与 $[x, y] \neq 1$ 矛盾. 这再一次推出 $\langle x, y\rangle \cong \mathrm{D}_8$. 故 G 是 $\mathcal{T}_3$ 群.

情形 2 G 至少有一个子群 $Q = \langle a, b\rangle \cong \mathrm{Q}_8$.

首先我们断言: $\mho_1(G) = G'$ 且是 2 阶的. 否则, 对 G 的任意 4 阶元 g, 设 $g^2 \neq a^2 = b^2$. 则 $|\langle g, a\rangle| > 8$, 因而 $[g, a] = 1$. 类似地, $[g, b] = 1$. 令 $H = \langle ga, b\rangle$. 因为 $(ga)^2 = g^2a^2 \neq b^2$, 故 $|H| > 8$. 这矛盾于 $[ga, b] \neq 1$. 于是 $|\mho_1(G)| = 2$. 另一方面, 注意到 $G' = \langle [x, y] \mid x, y \in G\rangle$. 若 $[x, y] \neq 1$, 则 $\langle x, y\rangle \cong \mathrm{D}_8$ 或 Q_8. 在任何情况下, $[x, y] \in \mho_1(\langle x, y\rangle) \leqslant \mho_1(G)$. 于是断言成立. 由此可得: G/G' 是初等交换的.

由引理 10.5.1 可得, $G = E * A$, 其中 E 是超特殊群, A 是交换的. 若 A 是初等交换的, 则 $A \leqslant Z(G)$. 因为 G 是基本的 $\mathcal{T}_3$ 群, 故 $A \leqslant E$, 因而 $G = E$. 若 A 不初等交换且 G 是基本的 $\mathcal{T}_3$ 群, 再由引理 10.5.1 可得, $\mho_1(A) = E \bigcap A = Z(E)$. 由此可得 $A \cong \mathrm{C}_4$. 故 $G = E * \mathrm{C}_4$.

为了结束 (1) 的证明, 我们需要证明 E 和 $E * \mathrm{C}_4$ 是 $\mathcal{T}_3$ 群. 明显地, 超特殊群 E 是 $\mathcal{T}_3$ 群. 假设 $G = E * \mathrm{C}_4$. 令 $a, b \in G$ 且 $[a, b] \neq 1$. 再令 $a = a_1c^i$ 且 $b = b_1c^j$, 其中 $a_1, b_1 \in E$, $c \in Z(G)$ 且 $i, j = \pm 1$. 则 $[a_1, b_1] \neq 1$. 易验证, 若 $\langle a_1, b_1\rangle \cong \mathrm{Q}_8$, 则 $\langle a, b\rangle \cong \mathrm{D}_8$. 若 $\langle a_1, b_1\rangle \cong \mathrm{D}_8$, 则 $\langle a, b\rangle \cong \mathrm{D}_8$ 或 Q_8. 结论得证.

假设 $p \geqslant 3$. 因为 $\exp(G) = p^2$, G 有子群与 $\mathrm{M}_p(2, 1)$ 同构. 注意到 $\mathrm{M}_p(2, 1)$ 可以由两个 p^2 阶元生成且这两个元的 p 次方相等. 与 $p = 2$ 的情形 (2) 的论证类似, 我们也可得 $\mho_1(G) = G'$ 且是 p 阶的 (计算细节省略).

由引理 10.5.1 及与 (1) 的情形 2 相同的论证可得: $G = E$ 或 $G = E * \mathrm{C}_{p^2}$. 反之, 若 $G = E$ 或 $G = E * \mathrm{C}_{p^2}$, 易验证 G 是 $\mathcal{T}_3$ 群. 验证留给读者. $\square$

总结以上的论述, 我们有如下定理.

定理 10.5.6　设 G 是 $\mathcal{T}_3$ 群. 则 G 是定理 10.5.3 中的群或是一个初等交换 p 群与定理 10.5.5 中的任一个群的直积.

作为定理 10.5.6 的直接推论, 我们有如下定理.

定理 10.5.7　设 G 是 p 群且 G 满足条件: 对于所有的 $x,y\in G$, $|\langle x,y\rangle|\leqslant p^3$. 则 G 是下列群之一.

(1) 交换群 C_{p^3}, $\mathrm{C}_{p^2}\times\mathrm{C}_p^n$ 或 C_p^n, n 为正整数;

(2) 定理 10.5.3 中的群;

(3) 一个初等交换 p 群与定理 10.5.5 中的任一个群的直积, 但对于定理 10.5.5(1) 中的广义二面体群, $s=1$.

10.6　两个非交换元生成 p^4 阶内交换子群的 p 群

继 $\mathcal{T}_3$ 群分类之后, 安立坚等在文献 [7] 分类了 $\mathcal{T}_4$ 群, 即两个非交换元生成 p^4 阶内交换子群的有限 p 群. 余大鹏等在文献 [250] 研究了两类这样的有限 p 群 G, 一类是: 对任意的 $x,y\in G$ 都有 $|\langle x,y\rangle|\leqslant p^i\cdot\max\{|x|,|y|\}$. 另一类是: 对任意的 $x,y\in G$ 都有 $|\langle x,y\rangle|\leqslant p^i|x|$. 他们给出了这两类群的幂零类、导群的方次数等结果. 本节的内容取自 [7].

由定理 1.7.7 和定理 1.7.10 直接可得下列结论.

引理 10.6.1　G 是 p^4 阶的内交换群当且仅当 G 是下列互不同构的群之一.

(1) $\mathrm{M}_p(3,1)$, 此时 $\exp(G)=p^3$, $\Phi(G)=\mho_1(G)\cong\mathrm{C}_{p^2}$, $\Omega_1(G)\cong\mathrm{C}_p^2$;

(2) $\mathrm{M}_p(2,2)$, 此时 $\exp(G)=p^2$, $\Phi(G)=\mho_1(G)=\Omega_1(G)\cong\mathrm{C}_p^2$;

(3) $\mathrm{M}_p(2,1,1)$, 此时 $\exp(G)=p^2$, $\Omega_1(G)\cong\mathrm{C}_p^3$. 若 $p=2$, 则 $\Phi(G)=\mho_1(G)\cong\mathrm{C}_2^2$; 若 $G=\langle x,y\rangle$, 其中 x,y 均为 4 阶元, 则 $\mho_1(G)=\langle x^2,y^2\rangle$ 且 $[x,y]=x^2y^2$; 若 $p>2$, 则 $\Phi(G)\cong\mathrm{C}_p^2$ 且 $\mho_1(G)<\Phi(G)$.

利用 [23] 中的引理 5.2 的论证可得下列引理.

引理 10.6.2　设 E 是 p 群 G 的内交换子群. 若 $[G,E]=E'$, 则 $G=E*C_G(E)$.

注　[23] 中的引理 5.3 是比引理 10.6.2 更强的结果. 作者没有假设 E 是内交换的这个条件, 得到了与引理 10.6.2 相同的结果. 需要说明的是, 若没有 E 是内交换的这个条件, 则 [23] 中的引理 5.3 的结论不成立. 例如, 设 $G=\mathrm{Q}_8*\mathrm{Q}_8$ 且 $E=\mathrm{Q}_8*\mathrm{C}_4$. 则 $C_G(E)\leqslant E$ 且 $E*C_G(E)\leqslant E$. 于是 $G\neq E*C_G(E)$.

定理 10.6.3　设 G 为 $\mathcal{T}_4$ 群. 则

(1) $\exp(G)\leqslant p^3$;

(2) $\mho_1(G)\leqslant Z(G)$;

(3) $\Omega_1(G)$ 交换;

(4) $c(G) = 2$;

(5) G' 初等交换;

(6) $C_G(a) \trianglelefteq G$ 对任意 $a \in G$;

(7) $G \times \mathrm{C}_p^n$ 为 $\mathcal{T}_4$ 群.

证明 (1) 若否, 存在 $g \in G$ 使得 $o(g) \geqslant p^4$. 由题设可知, $g \in Z(G)$. 由于 G 非交换, 故存在 $a, b \in G$ 使得 $\langle a, b\rangle$ 为 p^4 阶内交换群. 由题设及 $o(ag) = o(g)$ 可得, $ag \in Z(G)$. 因而 $a \in Z(G)$, 矛盾.

(2) 任取 $a, b \in G$, 若 $[a, b] = 1$, 则 $[a^p, b] = 1$; 若 $[a, b] \neq 1$, 则 $H = \langle a, b\rangle$ 为 p^4 阶内交换群. 由于 $\langle a^p, b\rangle < H$, 故 $[a^p, b] = 1$. 因此 $\mho_1(G) \leqslant Z(G)$.

(3) 由引理 10.6.1 可知, p^4 阶内交换群不能由 p 阶元生成. 因而 G 的任意两个 p 阶元交换. 所以, $\Omega_1(G)$ 交换.

(4) 首先, 我们断言: 对任意 $a, b \in G$, 有 $[a, b, b] = 1$. 若 $[a, b] = 1$, 显然结论成立. 若 $[a, b] \neq 1$, 则 $H = \langle a, b\rangle$ 为 p^4 阶内交换群. 因而 $[a, b] \in Z(H)$, 且 $[a, b, b] = 1$.

由 [89] 中的III, 定理 6.5 可得, $c(G) \leqslant 3$, 且若 G 中无 3 阶元, 则 $c(G) \leqslant 2$. 若 $c(G) = 3$, 则 $p = 3$ 且存在 $x, y, z \in G$ 使得 $[x, y, z] \neq 1$. 令 $H = \langle x, y\rangle$. 则 H 为 p^4 阶内交换群. 由于 $H' \nleqslant Z(G)$, 由 (2) 可知, $H' \nleqslant \mho_1(H)$. 再由引理 10.6.1 可得, $H \cong \mathrm{M}_3(2, 1, 1)$. 令

$$H = \langle a, b, c | a^9 = b^3 = c^3 = 1, [a, b] = c, [a, c] = [b, c] = 1\rangle.$$

则 $[a, b, z] \neq 1$. 由于 $[a, bz, bz] = [a, b, b][a, b, z][a, z, b][a, z, z]$, 故 $[a, b, z][a, z, b] = 1$, 进而 $[a, z, b] \neq 1$. 同理可证, $\langle a, z\rangle \cong \mathrm{M}_3(2, 1, 1)$. 由于 $o([a, z]) = 3$ 且 $o(b) = 3$, 由 (3) 可得, $[a, z, b] = 1$, 矛盾.

(5) 设 $x, y \in G$ 且 $[x, y] \neq 1$, 则 $\langle x, y\rangle$ 为 p^4 阶内交换群. 由定理 1.7.7 可得, $o([x, y]) = p$. 由 (4) 可知, $G' \leqslant Z(G)$. 因此, $G' = \langle [x, y] \mid x, y \in G\rangle$ 为初等交换群.

(6) 任取 $x \in C_G(a)$, $y \in G$, 由 (4) 可知, $[x, y] \in G' \leqslant Z(G) \leqslant C_G(a)$. 因此, $x^y = x[x, y] \in C_G(a)$. 故 $C_G(a) \trianglelefteq G$.

(7) 令 $K = G \times C$, 其中 $C \cong \mathrm{C}_p^n$. 任取 $x = ac_1$, $y = bc_2$, 其中 $a, b \in G$, c_1, $c_2 \in C$. 设 $H = \langle x, y\rangle$ 和 $M = \langle a, b\rangle$. 若 H 非交换, 则 M 也非交换. 由 $\mathcal{T}_4$ 群的定义可知, M 为 p^4 阶内交换群. 由于 $\Phi(H) = \Phi(M)$, 故 H 也为 p^4 阶内交换群. 因此 K 为 $\mathcal{T}_4$ 群. □

为了分类 $\mathcal{T}_4$ 群, 由引理 10.6.1 可知, 我们需分以下四种情形讨论:

(1) 存在 G 的子群同构于 $\mathrm{M}_p(3, 1)$;

(2) G 的任意两个非交换元生成的子群同构于 $\mathrm{M}_p(2, 1, 1)$;

(3) G 的任意两个非交换元生成的子群同构于 $\mathrm{M}_p(2, 2)$;

(4) 存在 G 的两个子群分别同构于 $\mathrm{M}_p(2,1,1)$ 和 $\mathrm{M}_p(2,2)$, 且 G 中不存在子群同构于 $\mathrm{M}_p(3,1)$.

定理 10.6.4 *设 G 为 T_4 群. 若 G 中存在子群同构于 $\mathrm{M}_p(3,1)$, 则*

(1) 若 $a \in G$ 且 $o(a)=p^3$, 则 $\langle a\rangle \trianglelefteq G$;

(2) $G \cong \mathrm{M}_p(3,1)\times \mathrm{C}_p^n$.

证明 (1) 任取 $b\in G$, 若 $[a,b]=1$, 则 b 正规化 $\langle a\rangle$. 若 $[a,b]\neq 1$, 由引理 10.6.1 可知, $\langle a,b\rangle \cong \mathrm{M}_p(3,1)$. 由于 $o(a)=p^3$, 故 $\langle a\rangle \trianglelefteq \langle a,b\rangle$, 因而 b 正规化 $\langle a\rangle$. 由 b 的任意性可得, $\langle a\rangle \trianglelefteq G$.

(2) 设 $H\leqslant G$ 且 $H\cong \mathrm{M}_p(3,1)$. 不妨设 $H=\langle a,b \mid a^{p^3}=b^p=1,[a,b]=a^{p^2}\rangle$.

我们断言 $G=H*C_G(H)$. 由 (1) 可知, $\langle a\rangle \trianglelefteq G$ 且 $\langle ab\rangle \trianglelefteq G$. 由定理 10.6.3(5) 可得, $\exp(G')=p$. 任取 $x\in G$, 则 $[a,x]\in \Omega_1(\langle a\rangle)=H'$ 且 $[ab,x]\in\Omega_1(\langle ab\rangle)=H'$. 由于 $c(G)=2$ 且 $H=\langle a,ab\rangle$, 故 $[H,x]\leqslant H'$. 由 x 的任意性可得, $[H,G]\leqslant H'$. 由引理 10.6.2 可得, $G=H*C_G(H)$.

下证: $\exp(C_G(H))\leqslant p^2$. 若否, 则存在 p^3 阶元 $c\in C_G(H)$. 令 $K=\langle a,bc\rangle$. 则 K 非交换且 $\exp(K)\geqslant p^3$. 由引理 10.6.1 可知, $K\cong \mathrm{M}_p(3,1)$ 且 $\Phi(K)=\mho_1(K)$ 为 p^2 阶循环群. 因而 $\langle a^p\rangle=\langle c^p\rangle=\Phi(K)$. 令 $a^p=c^{tp}$, 其中 $(t,p)=1$. 由于 $(ac^{-t})^p=1$, 由定理 10.6.3(3) 可得, $[ac^{-t},b]=1$, 进而 $[a,b]=1$, 矛盾. 故 $\exp(C_G(H))\leqslant p^2$.

断言 $C_G(H)$ 交换. 若否, 则存在 $K\leqslant C_G(H)$ 且 K 为 p^4 阶内交换群. 由于 $\exp(C_G(H))\leqslant p^2$, 故 K 同构于 $\mathrm{M}_p(2,2)$ 或 $\mathrm{M}_p(2,1,1)$. 若 $K\cong \mathrm{M}_p(2,1,1)$, 令

$$K=\langle c,d \mid c^{p^2}=d^{p^2}=1,[c,d]=c^p\rangle,\quad M=\langle ac,d\rangle.$$

由于 M 非交换且 $\exp(M)\geqslant p^3$, 由引理 10.6.1 可知, $M\cong \mathrm{M}_p(3,1)$ 且 $\Phi(M)$ 为 p^2 阶循环群. 另外, 由于 $[ac,d]=[c,d]=c^p\in\Phi(M)$, 故 $\langle c^p,d^p\rangle\leqslant \Phi(M)$ 为 p^2 阶初等交换群, 矛盾. 若 $K\cong \mathrm{M}_p(2,1)$, 令

$$K=\langle c,d \mid c^{p^2}=d^p=e^p=1,[c,d]=e,[e,c]=[e,d]=1\rangle,\quad N=\langle ad,c\rangle.$$

由于 N 非交换且 $\exp(N)\geqslant p^3$, 由引理 10.6.1 可知, $N\cong \mathrm{M}_p(3,1)$ 且 $\Phi(N)$ 为 p^2 阶循环群. 另外, 由于 $[c,ad]=[c,d]=e\in\Phi(N)$, 故 $\langle c^p,e\rangle\leqslant\Phi(N)$ 为 p^2 阶初等交换群, 矛盾. 因此 $C_G(H)$ 交换.

由于 $a^p\in C_G(H)$ 且 $\exp(C_G(H))\leqslant p^2$, 故

$$C_G(H)=\langle a^p\rangle\times C \quad 且 \quad G=H*C_G(H)=H\times C.$$

下证 C 为初等交换群. 若否, 则 C 中存在 p^2 阶元 c. 令 $L=\langle a,bc\rangle$. 由于 L 非交换且 $\exp(L)\geqslant p^3$, 由引理 10.6.1 可得, $L\cong\mathrm{M}_p(3,1)$ 且 $\Phi(L)$ 为 p^2 阶循环群. 另外, 由于 $(bc)^p=c^p$, 故 $\langle a^p,c^p\rangle$ 为 $\Phi(L)$ 的 p^3 阶子群, 矛盾.

综上所证, $G \cong \mathrm{M}_p(3,1) \times \mathrm{C}_p^n$. 反之, 由定理 10.6.3(7) 可知, $\mathrm{M}_p(3,1) \times \mathrm{C}_p^n$ 为 $\mathcal{T}_4$ 群. □

引理 10.6.5 设 G 为 $\mathcal{T}_4$ 群. 若 G 中存在子群同构于 $\mathrm{M}_p(2,1,1)$, 且 G 中不存在子群同构于 $\mathrm{M}_p(3,1)$, 则 $\exp G = p^2$; 进一步地, 若 G 的任意两个非交换元生成的子群同构于 $\mathrm{M}_p(2,1,1)$, 则

(i) $C_G(a) = \langle a \rangle \times C$, 其中 C 初等交换;

(ii) 对任意的 $y \in G \backslash C_G(a)$, 存在 p 阶元 x 使得 $xC_G(a) = yC_G(a)$.

证明 不妨设

$$\mathrm{M}_p(2,1,1) = \langle a, b \mid a^{p^2} = b^p = c^p = 1, [a,b] = c, [c,a] = [c,b] = 1 \rangle.$$

若 $\exp(G) \neq p^2$, 则存在 $g \in G$ 使得 $o(g) = p^3$. 由引理 10.6.1(3) 可知, $g \in Z(G)$. 由于 $o(bg) \geqslant p^3$, 同理可知 $bg \in Z(G)$. 因而 $b \in Z(G)$, 与 $[a,b] \neq 1$ 矛盾.

若 G 的任意两个非交换元生成的子群同构于 $\mathrm{M}_p(2,1,1)$, 首先断言 $C_G(a)$ 交换. 若否, 则存在 $K \leqslant C_G(a)$ 且 $K \cong \mathrm{M}_p(2,1,1)$. 令

$$K = \langle x, y \mid x^{p^2} = y^p = z^p = 1, [x,y] = z, [z,x] = [z,y] = 1 \rangle, \quad M = \langle x, ay \rangle.$$

由于 M 非交换, 故 $M \cong \mathrm{M}_p(2,1,1)$ 且 $\Phi(M) = \langle x^p, z \rangle$. 由于 $a^p = (ay)^p \in \Phi(M)$, 可设 $a^p = x^{ip}z^j$. 令 $N = \langle ax^{-i}, y \rangle$. 由于 $\langle ax^{-i} \rangle \trianglelefteq N$, 故 $|N| \leqslant p^3$ 且 N 交换. 从而 $a^p = z^j$ (显然 $(j,p) = 1$). 若 $p = 2$, 则 $M \cong \mathrm{M}_2(2,2)$, 矛盾; 若 $p > 2$, 则 $\mho_1(M) = \langle x^p, a^p \rangle = \Phi(M)$, 与引理 10.6.1(3) 矛盾. 因而 $C_G(a)$ 交换.

由于 $\exp(C_G(a)) = p^2$, 可设 $C_G(a) = \langle a \rangle \times C$. 若 C 非初等交换, 则 C 中存在 p^2 阶元 w. 若 $[w,b] = 1$, 令 $L = \langle a, wb \rangle$, 则 L 非交换且 $\Phi(L) = \mho_1(L) = \langle a^p, w^p \rangle$. 由引理 10.6.1(3) 可知, $p = 2$ 且 $[a, wb] = c = a^2w^2 = (aw)^2$. 因而 $\langle aw, b \rangle \cong \mathrm{D}_8$, 矛盾. 若 $[w,b] \neq 1$ 且 $p > 2$, 由引理 10.6.1(3) 可知, $\langle ab, w \rangle \ncong \mathrm{M}_p(2,1,1)$, 矛盾. 若 $[w,b] \neq 1$ 且 $p = 2$, 则 $\langle ab, w \rangle$ 非交换. 由引理 10.6.1(3) 可知,

$$[ab, w] = [b, w] = (ab)^2w^2 = a^2w^2c.$$

因而 $\langle aw, b \rangle \cong \mathrm{D}_8$, 矛盾. 故 (i) 成立.

由于 $y \notin C_G(a)$, 故 $\langle a, y \rangle \cong \mathrm{M}_p(2,1,1)$. 令

$$\langle a, y \rangle = \langle a, b_1 \mid a^{p^2} = b_1^p = c_1^p = 1, [a, b_1] = c_1, [c_1, a] = [c_1, b] = 1 \rangle.$$

则可设 $y = a^i b_1^j c_1^k$, 其中 $(j,p) = 1$. 令 $x = b_1^j$, 则 $xC_G(a) = yC_G(a)$. 故 (ii) 成立. □

定理 10.6.6 设 G 为 $\mathcal{T}_4$ 群. 若 G 的任意两个非交换元生成的子群同构于 $\mathrm{M}_p(2,1,1)$, 则 $G \cong H \times \mathrm{C}_p^n$, 其中 $H = K \rtimes \langle a \rangle$, $K = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_k \rangle \times \langle c_1 \rangle \times \langle c_2 \rangle \times \cdots \times \langle c_k \rangle \cong \mathrm{C}_p^{2k}$, $a^{p^2} = 1$ 且 $b_i^a = b_i c_i$, $c_i^a = c_i$, $1 \leqslant i \leqslant k$.

证明　不妨设

$$\mathrm{M}_p(2,1,1)=\langle a,b_1 \mid a^{p^2}=b_1^p=c_1^p=1,[a,b_1]=c_1,[c_1,a]=[c_1,b_1]=1\rangle.$$

由定理 10.6.3(6) 可知, $C_G(a)\trianglelefteq G$. 令 $G/C_G(a)=\langle \bar{y}_1,\bar{y}_2,\cdots,\bar{y}_m\rangle$. 由引理 10.6.5(3) 可知, 存在 p 阶元 $x_1,x_2,\cdots,x_m$ 使得

$$G/C_G(a)=\langle \bar{x}_1,\bar{x}_2,\cdots,\bar{x}_m\rangle.$$

再令

$$M=\langle x_1,x_2,\cdots,x_m\rangle.$$

由定理 10.6.3(3) 可知, $M\leqslant \Omega_1(G)$ 交换. 令 $M=(M\bigcap C_G(a))\times N$. 则 $G=C_G(a)M=C_G(a)\rtimes N$. 设 $\varphi: N\to C_G(a)$ 满足 $\varphi(n)=[n,a],\forall n\in N$. 由于 $N\bigcap C_G(a)=1$, 故 φ 为单射, 因而 $[N,a]=\varphi(N)\cong N$. 由于 G 的 p^3 阶子群均交换, 故 $[N,a]\bigcap\langle a\rangle=1$, 因而 $\langle a\rangle\times[N,a]$ 为 $C_G(a)$ 的直积因子. 令

$$N=\langle b_1\rangle\times\langle b_2\rangle\times\cdots\times\langle b_k\rangle,\quad [b_i,a]=c_i,$$

其中 $1\leqslant i\leqslant k$. 则 $G'=[N,a]=\langle c_1\rangle\times\langle c_2\rangle\times\cdots\times\langle c_k\rangle$. 令 $K=N\times G'$. 则 $K\rtimes\langle a\rangle$ 满足 $b_i^a=b_ic_i$ 且 $c_i^a=c_i$, 其中 $1\leqslant i\leqslant k$. 令 $C_G(a)=\langle a\rangle\times G'\times E$. 则 E 初等交换且 $G=(K\rtimes\langle a\rangle)\times E$. 易证 $H=K\rtimes\langle a\rangle$ 为 $\mathcal{T}_4$ 群, 由定理 10.6.3(7) 可知, G 为 $\mathcal{T}_4$ 群. □

定理 10.6.7　*设 G 为 $\mathcal{T}_4$ 群. 若 G 的任意两个非交换元生成的子群同构于 $\mathrm{M}_p(2,2)$, 其中 $p>2$. 则 $G\cong H\times \mathrm{C}_p^n$, 其中 $H=K\rtimes\langle b\rangle$, $K=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_k\rangle\cong \mathrm{C}_{p^2}^k$, $o(b)=p^2$ 且对 $1\leqslant i\leqslant k$ 有 $a_i^b=a_i^{1+p}$.*

证明　用 H_m 表示群 $K\rtimes\langle b\rangle$, 其中 $K=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_m\rangle\cong \mathrm{C}_{p^2}^m$, $o(b)=p^2$ 满足: 对 $1\leqslant i\leqslant m$, $a_i^b=a_i^{1+p}$. 由题设可知, 存在 G 的子群同构于 $\mathrm{M}_p(2,2)$. 不妨设 $\mathrm{M}_p(2,2)=\langle a,b \mid a^{p^2}=b^{p^2}=1,[a,b]=a^p\rangle$. 显然, $\mathrm{M}_p(2,2)\cong H_1$. 令 $H=H_k$ 为 G 的满足 k 最大的子群.

首先断言 $\mho_1(G)=\mho_1(H)=\Omega_1(H)$. 同定理 10.6.3(1) 可证 $\exp(G)=p^2$. 因而只需证对任意 $g\in G$ 有 $g^p\in H$. 否则, 存在 $g\in G$ 使得 $g^p\notin H$. 对任意的 $a\in K\backslash\mho_1(K)$, 若 $[a,g]\neq 1$, 则由题设可知, $\langle a,g\rangle\cong \mathrm{M}_p(2,2)$. 因而, 不论 $[a,g]$ 是否为 1, 我们总可设 $[a,g]=a^{ip}g^{jp}$. 若 $(j,p)=1$, 由 $[a,bg]=a^{(1+ip)}g^{jp}\neq 1$ 可知, $\langle a,bg\rangle\cong \mathrm{M}_p(2,2)$. 另一方面, $\mho_1(\langle a,bg\rangle)\geqslant\langle a^p,b^p,g^p\rangle\cong \mathrm{C}_p^3$, 与引理 10.6.1 矛盾. 因而, 我们可设 $[a_l,g]=a_l^{i_lp}$, 其中 $1\leqslant l\leqslant k$, $0\leqslant i_l\leqslant p-1$. 若 $i_1\neq i_2$, 由 $[a_1a_2,g]=a_1^{i_1p}a_2^{i_2p}\neq 1$ 可知, $\langle a_1a_2,g\rangle\cong \mathrm{M}_p(2,2)$. 另一方面, $\mho_1(\langle a_1a_2,g\rangle)\geqslant\langle a_1^p,a_2^p,g^p\rangle\cong \mathrm{C}_p^3$, 与引理 10.6.1 矛盾. 因此 $i_1=i_2$. 同理可知, $i_1=i_2=\cdots=i_k$.

设 $a_{k+1}=gb^{-i_1}$, 则 $[a_1,a_{k+1}]=1$ 且 $a_{k+1}^p\notin H$. 若 $[a_{k+1},b]\neq 1$, 则由题设可知, $\langle a_{k+1},b\rangle\cong \mathrm{M}_p(2,2)$. 因而, 不论 $[a_{k+1},b]$ 是否为 1, 总有 $[a_{k+1},b]\in\langle a_{k+1}^p,b^p\rangle$. 同理可知, $[a_{k+1},b]=[a_{k+1},a_1b]\in\langle a_{k+1}^p,a_1^pb^p\rangle$. 因此, $[a_{k+1},b]\in\langle a_{k+1}^p\rangle$. 设 $[a_{k+1},b]=a_{k+1}^{sp}$, 其中 $0\leqslant s\leqslant p-1$. 若 $s=1$, 则 $\langle H,a_{k+1}\rangle\cong H_{k+1}$, 与 k 的选取矛盾. 若 $s\neq 1$, 设 $T=\langle a_1a_{k+1},b\rangle$, 由于 $[a_1a_{k+1},b]=a_1^pa_{k+1}^{sp}\neq 1$, 故 $T\cong \mathrm{M}_p(2,2)$. 另一方面, 由 $\Phi(T)\geqslant\langle a_1^pa_{k+1}^p,b^p,a_1^pa_{k+1}^{sp}\rangle=\langle a_1^p,a_{k+1}^p,b^p\rangle$ 可知, $|\Phi(T)|\geqslant p^3$, 与引理 10.6.1(2) 矛盾. 于是我们证得 $\mho_1(G)=\mho_1(H)=\Omega_1(H)$.

由引理 10.6.1(2) 可知, 对任意的 $u,v\in G$, 只要 $[u,v]\neq 1$, 就有 $[u,v]\in\Phi(\langle u,v\rangle)=\mho_1(\langle u,v\rangle)\leqslant H$. 因此 $H\trianglelefteq G$. 设 $G/H=\langle\bar{y}_1,\bar{y}_2,\cdots,\bar{y}_n\rangle$. 由 $\mho_1(G)=\mho_1(H)=\Omega_1(H)$ 可知, 存在 $h_i\in H$ 使得 $y_i^p=h_i^p$. 令 $x_i=y_ih_i^{-1}$, 则 $x_i^p=1$ 且 $G/H=\langle\bar{x}_1,\bar{x}_2,\cdots,\bar{x}_n\rangle$. 设 $E=\langle x_1,x_2,\cdots,x_n\rangle$. 由定理 10.6.3(3) 可知, $E\leqslant\Omega_1(G)$ 为初等交换群. 显然 $G=H\times E$. 易证 $H=K\rtimes\langle b\rangle$ 为 $\mathcal{T}_4$ 群, 由定理 10.6.3(7) 可知, G 为 $\mathcal{T}_4$ 群. □

引理 10.6.8 设 G 为 $\mathcal{T}_4$ 群. 若 G 的任意两个非交换元生成的子群同构于 $\mathrm{M}_2(2,2)$, 则

(1) $\exp(G)=2^2$;

(2) 对任意的 $a,b\in G$, 若 $[a,b]\neq 1$ 且 $a^2\neq b^2$, 则 $[a,b]=a^2$ 或 b^2;

(3) $\Omega_1(G)=Z(G)$.

证明 (1) 若否, 则存在 $g\in G$ 使得 $o(g)=2^3$. 由题设可知, $g\in Z(G)$. 由于 G 非交换, 故存在 $a,b\in G$ 使得 $\langle a,b\mid a^4=b^4=1,[a,b]=a^2\rangle\cong\mathrm{M}_2(2,2)$. 同理可知, $ag\in Z(G)$. 因而 $a\in Z(G)$, 与 $[a,b]\neq 1$ 矛盾.

(2) 由于 $[a,b]\neq 1$, 故 $\langle a,b\rangle\cong\mathrm{M}_2(2,2)$. 由引理 10.6.1 可知, $\Omega_1(\langle a,b\rangle)=\Phi(\langle a,b\rangle)=\langle a^2,b^2\rangle$, 因而 $[a,b]\in\langle a^2,\,b^2\rangle$. 若 $[a,b]=a^2b^2$, 则 $(ab)^2=a^2b^2[a,b]=1$, 进而有 $ab\in\Omega_1(\langle a,b\rangle)=\Phi(\langle a,b\rangle)$, 矛盾. 因此, $[a,b]=a^2$ 或 b^2.

(3) 首先断言 $\Omega_{\{1\}}(G)\subseteq Z(G)$. 否则, 存在 $a\in\Omega_{\{1\}}(G)$ 且 $b\in G$ 使得 $[a,b]\neq 1$. 由题设可知, $\langle a,b\rangle\cong\mathrm{M}_2(2,2)$. 由引理 10.6.1 可知, $\Omega_1(\langle a,b\rangle)=\Phi(\langle a,b\rangle)$. 因此 $a\in\Phi(\langle a,b\rangle)$, 矛盾.

由于 $\Omega_1(G)=\Omega_{\{1\}}(G)$, 所以 $\Omega_1(G)\leqslant Z(G)$. 要证 $\Omega_1(G)=Z(G)$, 只需证 $\exp(Z(G))=2$. 否则, 存在 $g\in Z(G)$ 使得 $o(g)=4$. 由题设可知, G 中存在子群 $\langle a,b\mid a^4=b^4=1,[a,b]=a^2\rangle\cong\mathrm{M}_2(2,2)$. 由于 $[ag,b]=a^2\neq 1$, $(ag)^2$ 或 b^2, 由 (2) 可知, $(ag)^2=b^2$, 进而 $g^2=a^2b^2$. 因此 $\langle a,gb\rangle\cong\mathrm{Q}_8$, 矛盾. □

定理 10.6.9 设 G 为 $\mathcal{T}_4$ 群, 若 G 的任意两个非交换元生成的子群同构于 $\mathrm{M}_2(2,2)$, 则 G 为下列互不同构的群之一.

(1) $H\times\mathrm{C}_2^n$, 其中 $H=K\rtimes\langle b\rangle$, $K=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_k\rangle\cong\mathrm{C}_4^k$, $b^4=1$ 且 $a_i^b=a_i^{-1}$ $(1\leqslant i\leqslant k)$;

(2) $H \times C_2^n$, 其中 $H = \langle a_1, a_2, b \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2 \rangle$;

(3) $H \times C_2^n$, 其中 $H = \langle a_1, a_2, b, d \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, d^2 = a_2^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2, [a_1, d] = a_1^2, [a_2, d] = a_1^2 a_2^2, [b, d] = 1 \rangle$.

证明　设 H 为 G 的极大阶交换子群. 由引理 10.6.8(1) 可设, $H = A \times C$, 其中 $A = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_k \rangle \cong C_4^k$ 且 C 初等交换. 由 H 的选法及引理 10.6.8(3) 可知, $Z(G) = \Omega_1(G) = \Omega_1(H) = \Omega_1(A) \times C$. 又由定理 10.6.3(2) 和 (5) 可得, $G' \leqslant \Omega_1(H)$ 且 $G/\Omega_1(H)$ 为初等交换群.

断言 1　对任意的 $g \in G \setminus H$ 和 $1 \leqslant i \leqslant k$, 有 $[a_i, g] \neq 1$.

若否, 不妨设 $[a_1, g] = 1$. 由 H 的选法可知, 存在 $h \in H$ 使得 $[h, g] \neq 1$. 令 $B = \langle h, a_1, g \rangle$. 易见 $a_1 \in Z(B)$. 另一方面, 由引理 10.6.8(3) 可得, $a_1 \notin \Omega_1(B) = Z(B)$, 矛盾.

断言 2　若对任意 $b \in G \setminus H$ 有 $b^2 \notin \mho_1(H)$, 则 G 同构于定理中的 (1) 型群.

此时, 对任意的 $1 \leqslant i \leqslant k$ 有 $b^2 \neq a_i^2$ 且 $(a_i b)^2 = a_i^2 b^2 [a_i, b] \neq a_i^2$. 因而 $[a_i, b] \neq b^2$. 由断言 1 可知, $[a_i, b] \neq 1$. 又由引理 10.6.8(2) 可得, $[a_i, b] = a_i^2$. 令 $d \in G \setminus H$. 同理可证, $[a_i, d] = a_i^2$. 由此推出 $[a_i, bd] = 1$ 且 $bd \in C_G(H)$. 由 H 的选取可知, $bd \in H$. 因而 $d \in \langle H, b \rangle$. 故 $G = \langle H, b \rangle$ 同构于定理中的 (1) 型群.

下面我们假设存在 $b \in G \setminus H$ 使得 $b^2 \in \mho_1(H)$. 不妨设 $b^2 = a_1^2$. 此时, $(ba_1)^2 = [a_1, b] \neq a_1^2$.

若 $k = 1$, 令 $L = \langle ba_1, a_1^2, C \rangle$. 则 L 为 G 的极大阶交换子群. 我们断言: 对任意的 $d \in G \setminus L$, 均有 $d^2 \notin \mho_1(L)$. (从而由断言 2 可知, G 同构于定理中的 (1) 型群.) 若否, 存在 $d \in G \setminus L$ 使得 $d^2 = (ba_1)^2 \neq a_1^2$. 由断言 1 及引理 10.6.8(2) 可知, $[a_1, d] = a_1^2 = b^2$ 或 $[a_1, d] = d^2$. 若 $[a_1, d] = a_1^2 = b^2$ 且 $[b, d] = 1$, 则 $\langle b, d, C \rangle$ 为交换群, 与 H 的取法矛盾. 若 $[a_1, d] = a_1^2 = b^2$ 且 $[b, d] \neq 1$, 则由引理 10.6.8(2) 可知, $[b, d] = b^2$ 或 d^2. 若 $[b, d] = b^2$, 则 $[ba_1, d] = 1$, 因而 $\langle L, d \rangle$ 交换, 与 H 的取法矛盾; 若 $[b, d] = d^2$, 则 $[a_1 d, b] = 1$, 因而 $\langle b, a_1 d, C \rangle$ 交换, 与 H 的取法矛盾. 若 $[a_1, d] = d^2$, 同上可知, $[b, d] = b^2$ 或 d^2. 若 $[b, d] = b^2$, 则 $[a_1, bd] = 1$, 从而 $\langle H, bd \rangle$ 交换, 又与 H 的取法矛盾; 若 $[b, d] = d^2$, 则 $[ba_1, d] = 1$, 进而 $\langle ba_1, d, C \rangle$ 交换, 还与 H 的取法矛盾.

下面我们假设 $k \geqslant 2$. 由于 $b^2 = a_1^2 \neq a_2^2$, 由断言 1 和引理 10.6.8(2) 可知, $[a_2, b] = b^2 = a_1^2$ 或 a_2^2. 同理可证 $[a_1 a_2, b] = [a_1, b][a_2, b] = a_1^2$ 或 $a_1^2 a_2^2$. 因此 $[a_1, b] = a_2^2$ 或 $(a_1 a_2)^2$. 若 $k > 2$, 同理可证 $[a_1, b] = a_3^2$ 或 $(a_1 a_3)^2$, 矛盾. 因此 $k = 2$. 不妨设 $[a_1, b] = a_2^2$. 此时 $[a_2, b] = a_1^2$. 若 $G = \langle H, b \rangle$, 则 G 为定理中的 (2) 型群. 下设 $G \neq \langle H, b \rangle$.

断言 3　对任意的 $d \in G \setminus \langle H, b \rangle$ 有 $d^2 \in \{a_1^2, a_2^2, a_1^2 a_2^2\}$.

若否, 由引理 10.6.8(2) 及断言 1 可得, $[a_1, d] = a_1^2$ 或 d^2, $[a_2, d] = a_2^2$ 或 d^2, 且 $[a_1a_2, d] = a_1^2a_2^2$ 或 d^2. 由此可得 $[a_1, d] = a_1^2$ 且 $[a_2, d] = a_2^2$. 进而有 $[a_1a_2, bd] = 1$, 与断言 1 矛盾.

以下对 d^2 的三种可能的取值分情况讨论.

情形 1 $d^2 = a_2^2$.

由引理 10.6.8(2) 及断言 1 可知, $[a_1, d] = a_1^2$ 或 a_2^2 且 $[a_1a_2, d] = a_1^2a_2^2$ 或 a_2^2. 因此 $[a_2, d] = a_1^2$ 或 $a_1^2a_2^2$. 若 $[a_2, d] = a_1^2$, 则 $[a_2, bd] = 1$, 与断言 1 矛盾. 因此 $[a_2, d] = a_1^2a_2^2$, 此时 $[a_1, d] = a_1^2$.

下证: $G = \langle H, b, d\rangle$. 若否, 存在 $f \in G \setminus \langle H, b, d\rangle$. 由断言 3 可知, $f^2 \in \{a_1^2, a_2^2, a_1^2a_2^2\}$. 若 $f^2 = a_2^2$, 由断言 1 及引理 10.6.8(2) 可知, $[a_1, f] = a_1^2$ 或 a_2^2. 此时, $[a_1, df] = 1$ 或 $[a_1, bf] = 1$, 与断言 1 矛盾. 若 $f^2 = a_1^2$ 或 $a_1^2a_2^2$, 同理可得矛盾.

由于 $b^2 \neq d^2$, 由引理 10.6.8(2) 可知, $[b, d] = b^2$, 1 或 d^2. 若 $[b, d] = b^2$, 则 $\langle a_2, bd\rangle \cong Q_8$, 矛盾. 若 $[b, d] = 1$, 则 G 为定理中的 (3) 型群. 若 $[b, d] = d^2$, 用 a_1d 替换 d 可知, G 也为定理中的 (3) 型群.

情形 2 $d^2 = a_1^2$.

由于 $b^2 = a_1^2 = d^2$, 由断言 3 可知, $(bd)^2 = [b, d] \in \{a_1^2, a_2^2, a_1^2a_2^2\}$. 若 $(bd)^2 = a_1^2$, 则 $\langle b, d\rangle \cong Q_8$, 矛盾. 若 $(bd)^2 = a_2^2$, 用 bd 替换 d, 可转化为情形 1. 因此我们可设 $(bd)^2 = [b, d] = a_1^2a_2^2$. 由于 $(a_1a_2b)^2 = a_1^2 = d^2$, 同上可设 $[a_1a_2b, d] = a_1^2a_2^2$. 此时, $[a_1a_2, d] = 1$, 与断言 1 矛盾.

情形 3 $d^2 = a_1^2a_2^2$.

由断言 3 可知, $(a_1a_2d)^2 = [a_1a_2, d] \in \{a_1^2, a_2^2, a_1^2a_2^2\}$. 若 $(a_1a_2d)^2 = a_1^2a_2^2$, 则 $\langle a_1a_2, d\rangle \cong Q_8$, 矛盾. 因而 $(a_1a_2d)^2 = a_1^2$ 或 a_2^2. 用 a_1a_2d 替换 d, 可转化为情形 1 或情形 2.

由以上证明过程可知, 定理中的群互不同构. 易证 H 为 $\mathcal{T}_4$ 群, 由定理 10.6.3(7) 可知, G 为 $\mathcal{T}_4$ 群. □

由 $\mathcal{T}_4$ 群的定义可知, p^5 阶 $\mathcal{T}_4$ 群恰好是三元生成的 p^5 阶 $\mathcal{A}_2$ 群. 下面引理是文献 [273] 的直接结论.

引理 10.6.10 *设 G 为 p^5 阶 $\mathcal{T}_4$ 群. 则 G 为下列群之一.*

(1) $\langle a, b\rangle \times C_p$, 其中 $\langle a, b\rangle$ 为 p^4 阶内交换群;

(2) $\langle a, b\rangle * C_{p^2}$, 其中 $\langle a, b\rangle \cong M_p(2, 1, 1)$, 即 $G = \langle a, b, d \mid a^{p^2} = b^p = d^{p^2} = 1, [a, b] = d^p, [d, a] = [d, b] = 1\rangle$;

(3) $\langle a, b, c \mid a^4 = b^4 = 1, c^2 = a^2b^2, [a, b] = b^2, [c, a] = a^2, [c, b] = 1\rangle$;

(4) $\langle a, b\rangle \rtimes C_p$, 其中 $\langle a, b\rangle \cong M_p(2, 2)$, $p > 2$, 即 $G = \langle a, b, d \mid a^{p^2} = b^{p^2} = d^p = 1, [a, b] = a^p, [d, a] = b^p, [d, b] = 1\rangle$;

(5) $\langle a,b,d \mid a^p=b^{p^2}=d^{p^2}=1,[a,b]=d^p,[d,a]=b^{-\nu p},[d,b]=1\rangle$, 其中 $p>2$ 且 ν 为固定的模 p 的平方非剩余;

(6) $\langle a,b,d \mid a^p=b^{p^2}=d^{p^2}=1,[a,b]=d^p,[d,a]=b^{jp}d^p,[d,b]=1\rangle$. 若 $p>2$, 则 $4j=1-\rho^{2r+1}$, $1\leqslant\rho\leqslant\dfrac{p-1}{2}$, ρ 为模 p 的本原根中最小的正整数; 若 $p=2$, 则 $j=1$.

定理 10.6.11 设 G 为 $\mathcal{T}_4$ 群, G 有两个子群分别同构于 $\mathrm{M}_p(2,1,1)$ 和 $\mathrm{M}_p(2,2)$, 且无子群同构于 $\mathrm{M}_p(3,1)$. 再设 $H\leqslant G$ 满足: H 中没有子群同构于 $\mathrm{M}_p(2,2)$ 且 H 的阶最大. 则可设 $H=(K\rtimes\langle b\rangle)\times E$, 其中 $b^{p^2}=1$, $K=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_k\rangle\times\langle c_1\rangle\times\langle c_2\rangle\times\cdots\times\langle c_k\rangle\cong \mathrm{C}_p^{2k}$, $E\cong\mathrm{C}_p^n$, 且 $a_i^b=a_ic_i$, $c_i^b=c_i$, $1\leqslant i\leqslant k$. 进一步地,

(1) $\Omega_1(G)=\Omega_1(H)=K\times\langle b^p\rangle\times E$;

(2) $H\trianglelefteq G$ 且 G/H 初等交换;

(3) 若 $p>2$, 则对任意的 $d\in G\backslash H$, $1\leqslant i\leqslant k$, 有 $\langle d^p,b^p\rangle=\langle b^p,c_i\rangle$;

(4) 若 $p=2$, 则对任意的 $d\in G\backslash H$, $1\leqslant i\leqslant k$, 有 $d^2\in\{b^2,c_i,b^2c_i\}$;

(5) $k=1$;

(6) 若 $p=2$, 则对任意 $x\in G\backslash H$ 存在 $h\in H$ 使得 $d=xh$ 满足下列关系之一:

(i) $d^2=c_1$ 且 $[a_1,d]=[b,d]=1$,

(ii) $d^2=c_1,[b,d]=1$ 且 $[a_1,d]=b^2c_1$,

(iii) $d^2=c_1,[b,d]=b^2$ 且 $[a_1,d]=b^2$;

(7) $E\leqslant Z(G)$;

(8) H 为 G 的极大子群;

(9) $G\cong L\times\mathrm{C}_p^n$, 其中 L 为引理 10.6.10 中 (2), (4), (5) 或 (6) 型群之一.

证明 (1) 由定理 10.6.3(3) 可知, $\Omega_1(G)$ 为交换群. 由于 $\Omega_1(G)\trianglelefteq G$ 且 $b^p\in\Omega_1(G)$, 所以 $\Omega_1(G)\lessdot\Omega_1(G)\langle b\rangle$. 设 L 为 $\Omega_1(G)\langle b\rangle$ 的二元生成的非交换子群, 则 $L\bigcap\Omega_1(G)\lessdot L$, 进而 $|\Omega_1(L)|=p^3$. 由引理 10.6.1 可知, $L\cong\mathrm{M}_p(2,1,1)$. 因此, $\Omega_1(G)\langle b\rangle$ 中无子群同构于 $\mathrm{M}_p(2,2)$. 由 $|H|$ 的选取可得 $|\Omega_1(G)\langle b\rangle|\leqslant|H|$. 由于 $\Omega_1(H)\leqslant\Omega_1(G)$, 故 $H=\Omega_1(H)\langle b\rangle\leqslant\Omega_1(G)\langle b\rangle$. 因此 $\Omega_1(G)=\Omega_1(H)=K\times\langle b^p\rangle\times E$.

(2) 由定理 10.6.3 可知, $G'\leqslant\Omega_1(G)$. 同引理 10.6.8(1) 可证, $\exp(G)=p^2$. 因此 $\mho_1(G)\leqslant\Omega_1(G)$, 进而有 $\Phi(G)=G'\mho_1(G)\leqslant\Omega_1(G)\leqslant H$. 所以 $H\trianglelefteq G$ 且 G/H 初等交换.

(3) 首先断言 $d^p\notin\langle b^p\rangle$. 若否, 设 $d^p=b^{kp}$, 则 $(db^{-k})^p=1$. 因而 $db^{-k}\in\Omega_1(G)\leqslant H$. 故 $d\in H$, 矛盾. 用 A_l 表示群 $\langle a_i^ld,b\rangle$, 其中 $0\leqslant l\leqslant p-1$. 若 A_l 非交换, 则 A_l 为 p^4 阶群. 由于 $\mho_1(A_l)=\langle d^p,b^p\rangle$ 为 p^2 阶初等交换群, 由引理 10.6.1 可知, $A_l\cong\mathrm{M}_p(2,2)$. 特别地, 若 $[d,b]\neq1$, 则 $[d,b]\in\Phi(A_0)=\mho_1(A_0)=\langle d^p,b^p\rangle$.

由于 $[a_i^ld,b]=c_i^l[d,b]$, 所以存在 $1\leqslant s\leqslant p-1$, 使得 $A_s=\langle a_i^sd,b\rangle$ 非交换. 此

时, $[a_i^s d, b] = c_i^s [d, b] \in \Phi(A_s) = \mho_1(A_s) = \langle d^p, b^p \rangle$. 从而 $c_i \in \langle d^p, b^p \rangle = \Phi(A_s)$, 故 $\langle d^p, b^p \rangle = \langle b^p, c_i \rangle = \Phi(A_s)$.

(4) 由 (1) 可知, $\Omega_1(G) \leqslant H$. 由于 $d \notin H$, 故 $d \notin \Omega_1(G)$ 且 $d^2 \neq 1$. 若 $d^2 \notin \langle b^2, c_i \rangle$, 则 $|\langle d^2, b^2, c_i \rangle| \geqslant 2^3$.

若 $[b, d] = 1$, 令 $A = \langle a_i d, b \rangle$, 则 $[a_i d, b] = c_i \neq 1$. 因此 A 为 2^4 阶非交换群且 $\Phi(A) = \langle b^2, c_i \rangle$. 因而 $(a_i d)^2 = [a_i, d] d^2 \in \Phi(A)$. 令 $B = \langle a_i b, d \rangle$, 则 $|B| = 2^4$ 且 $\Phi(B) = \langle (a_i b)^2, d^2 \rangle = \langle b^2 c_i, d^2 \rangle$. 因此 $[a_i b, d] = [a_i, d] \in \Phi(B)$, 且 $[a_i, d] d^2 \in \Phi(B)$. 所以 $[a_i, d] d^2 \in \Phi(B) \bigcap \Phi(A) = \langle b^2 c_i \rangle$. 若 $[a_i, d] d^2 = 1$, 则 $\langle a_i, d \rangle \cong \mathrm{D}_8$, 矛盾. 若 $[a_i, d] d^2 = b^2 c_i$, 则 $\langle a_i, bd \rangle \cong \mathrm{D}_8$, 与 $\mathcal{T}_4$ 群的定义矛盾.

若 $\langle b, d \rangle \cong \mathrm{M}_2(2,1,1)$, 则由引理 10.6.1 可知, $[b, d] = b^2 d^2$. 因此 $(bd)^2 = 1$, 进而 $bd \in \Omega_1(G) \leqslant H$. 故 $d \in H$, 矛盾.

若 $\langle b, d \rangle \cong \mathrm{M}_2(2,2)$ 且 $[b, d] = d^2$, 令 $A = \langle a_i d, b \rangle$ 且 $B = \langle a_i b, d \rangle$, 则同上可证 $(a_i d)^2 = [a_i, d] d^2 \in \Phi(A) = \langle b^2, d^2 c_i \rangle$ 且 $[a_i b, d] = [a_i, d] d^2 \in \Phi(B) = \langle b^2 c_i, d^2 \rangle$. 因而 $[a_i, d] d^2 \in \Phi(B) \bigcap \Phi(A) = \langle d^2 b^2 c_i \rangle$. 若 $[a_i, d] d^2 = 1$, 则 $\langle a_i, d \rangle \cong \mathrm{D}_8$, 矛盾. 若 $[a_i, d] d^2 = d^2 b^2 c_i$, 则 $\langle a_i, bd \rangle \cong \mathrm{D}_8$, 矛盾.

若 $\langle b, d \rangle \cong \mathrm{M}_2(2,2)$ 且 $[b, d] = b^2$, 令 $A = \langle a_i d, b \rangle$ 且 $B = \langle a_i b, d \rangle$, 同上可证 $(a_i d)^2 = [a_i, d] d^2 \in \Phi(A) = \langle b^2, b^2 c_i \rangle$ 且 $[a_i b, d] = [a_i, d] b^2 \in \Phi(B) = \langle b^2 c_i, d^2 \rangle$. 因此 $[a_i, d] b^2 d^2 \in \Phi(A)$ 且 $[a_i, d] b^2 d^2 \in \Phi(B)$. 进而有 $[a_i, d] b^2 d^2 \in \Phi(B) \bigcap \Phi(A) = \langle b^2 c_i \rangle$. 若 $[a_i, d] b^2 d^2 = 1$, 设 $C = \langle a_i b, a_i d \rangle$. 由于 $[a_i b, a_i d] = b^2 d^2 c_i b^2 = d^2 c_i \neq 1$, 且 $\Phi(\langle a_i b, a_i d \rangle) = \langle b^2, b^2 c_i, d^2 c_i \rangle \cong \mathrm{C}_2^3$, 故 $|\langle a_i b, a_i d \rangle| \neq 2^4$, 矛盾. 若 $[a_i, d] b^2 d^2 = b^2 c_i$, 则 $\langle a_i, bd \rangle \cong \mathrm{D}_8$, 矛盾.

(5) 设 $k \geqslant 2$. 令 $d \in G \backslash H$. 若 $p > 2$, 则由 (3) 可得, $\langle d^p, b^p \rangle = \langle b^p, c_1 \rangle = \langle b^p, c_2 \rangle$ 矛盾. 若 $p = 2$, 则由 (4) 可知, $d^2 \in \{b^2, c_1, b^2 c_1\} \bigcap \{b^2, c_2, b^2 c_2\}$. 因而 $d^2 = b^2$. 由于 $db \notin H$, 同理可得 $(db)^2 = b^2$. 进而 $\langle b, d \rangle \cong \mathrm{Q}_8$, 与 $\mathcal{T}_4$ 群的定义矛盾.

(6) 由 (4) 可知, $x^2 \in \{b^2, c_1, b^2 c_1\}$. 下面对 x^2 的取值分情况讨论.

情形 1 $x^2 = c_1$.

若 $[b, x] \neq 1$, 则 $\langle b, x \rangle$ 为 16 阶内交换群. 因此 $[b, x] \in \Phi(\langle b, x \rangle) = \langle b^2, c_1 \rangle$.

子情形 1.1 $[b, x] = 1$.

令 $d = x$ 且 $A = \langle a_1 d, b \rangle$. 由于 $[a_1 d, b] = c_1 \neq 1$, 故 A 为 2^4 阶非交换群且 $\Phi(A) = \langle b^2, c_1 \rangle$. 因此 $(a_1 d)^2 d^2 = [a_1, d] \in \langle b^2, c_1 \rangle$. 若 $[a_1, d] = 1$, 则可得关系 (i). 若 $[a_1, d] = b^2 c_1$, 则可得关系 (ii). 若 $[a_1, d] = c_1$, 则 $\langle a_1, d \rangle \cong \mathrm{D}_8$, 矛盾. 若 $[a_1, d] = b^2$, 则 $\langle a_1, bd \rangle \cong \mathrm{D}_8$, 矛盾.

子情形 1.2 $[b, x] = b^2 c_1$.

由于 $(bx)^2 = 1$, 故 $bx \in \Omega_1(G) \leqslant H$. 因此 $x \in H$, 矛盾.

子情形 1.3 $[b, x] = b^2$.

令 $A = \langle a_1x, b\rangle$. 由于 $[a_1x, b] = b^2c_1 \neq 1$, 故 A 为 2^4 阶非交换群且 $\Phi(A) = \langle b^2, c_1\rangle$. 因此 $(a_1x)^2x^2 = [a_1, x] \in \langle b^2, c_1\rangle$. 若 $[a_1, x] = b^2$, 令 $d = x$, 则可得关系 (iii); 若 $[a_1, x] = b^2c_1$, 令 $d = bx$, 则可得关系 (iii); 若 $[a_1, x] = c_1$, 则 $\langle a_1, x\rangle \cong \mathrm{D}_8$, 与 $\mathcal{T}_4$ 群的定义矛盾. 若 $[a_1, x] = 1$, 则 $\langle a_1, bx\rangle \cong \mathrm{D}_8$, 与 $\mathcal{T}_4$ 群的定义矛盾.

子情形 1.4 $[b, x] = c_1$.

设 $B = \langle a_1b, x\rangle$, 则 $|B| = 2^4$ 且 $\Phi(B) = \langle b^2, c_1\rangle$. 因此 $[a_1b, x]c_1 = [a_1, x] \in \langle b^2, c_1\rangle$. 若 $[a_1, x] = 1$, 令 $x' = a_1x$, 则有 $x'^2 = c_1$ 且 $[b, x'] = 1$, 转化为子情形 1.1. 若 $[a_1, x] = b^2$, 令 $x' = a_1bx$, 则有 $x'^2 = c_1$ 且 $[b, x'] = 1$, 转化为子情形 1.1. 若 $[a_1, x] = c_1$, 则 $\langle a_1, x\rangle \cong \mathrm{D}_8$, 矛盾. 若 $[a_1, x] = b^2c_1$, 则 $\langle a_1, bx\rangle \cong \mathrm{D}_8$, 矛盾.

情形 2 $x^2 = b^2c_1$.

若 $[b, x] \neq 1$, 则 $\langle b, x\rangle$ 为 16 阶内交换群. 因而, $[b, x] \in \Phi(\langle b, x\rangle) = \langle b^2, c_1\rangle$.

子情形 2.1 $[b, x] = 1$.

令 $x' = bx$. 则 $x'^2 = c_1$, 转化为情形 1.

子情形 2.2 $[b, x] = b^2$.

令 $A = \langle a_1x, b\rangle$. 由于 $[a_1x, b] = b^2c_1 \neq 1$, 故 A 为 2^4 阶非交换群且 $\Phi(A) = \langle b^2, c_1\rangle$. 因此 $(a_1x)^2x^2 = [a_1, x] \in \langle b^2, c_1\rangle$. 若 $[a_1, x] = b^2$, 令 $x' = a_1x$, 则 $x'^2 = c_1$, 化为情形 2.1. 若 $[a_1, x] = b^2c_1$, 则 $\langle a_1, x\rangle \cong \mathrm{D}_8$, 矛盾. 若 $[a_1, x] = c_1$, 则 $\langle a_1b, x\rangle \cong \mathrm{Q}_8$, 矛盾. 若 $[a_1, x] = 1$, 则 $\langle a_1b, bx\rangle \cong \mathrm{Q}_8$, 矛盾.

子情形 2.3 $[b, x] = b^2c_1$.

设 $C = \langle a_1b, bx\rangle$, 则 $|C| = 2^4$ 且 $\Phi(C) = \langle b^2, c_1\rangle$. 因此 $[a_1b, bx]b^2 = [a_1, x] \in \langle b^2, c_1\rangle$. 若 $[a_1, x] = b^2$, 令 $x' = a_1x$, 则 $x'^2 = c_1$, 化为情形 2.1. 若 $[a_1, x] = 1$, 则 $\langle a_1b, x\rangle \cong \mathrm{Q}_8$, 矛盾. 若 $[a_1, x] = c_1$, 则 $\langle a_1x, b\rangle \cong \mathrm{Q}_8$, 矛盾. 若 $[a_1, x] = b^2c_1$, 则 $\langle a_1, bx\rangle \cong \mathrm{D}_8$, 矛盾.

子情形 2.4 $[b, x] = c_1$.

此时 $(bx)^2 = 1$. 因此 $bx \in \Omega_1(G) \leqslant H$. 进而 $x \in H$, 矛盾.

情形 3 $x^2 = b^2$.

断言 $(bx)^2 = [b, x] \neq b^2$. (否则, $\langle b, x\rangle \cong \mathrm{Q}_8$, 矛盾.) 令 $x' = bx$, 化为情形 1 或情形 2.

(7) 我们只需证明: 对任意的 $e \in E$ 和 $x \in G\backslash H$ 有 $[e, x] = 1$.

当 $p = 2$ 时, 由 (6), 存在 $h \in H$ 使得 $d = hx$ 满足关系 (i), (ii) 或 (iii). 由 (4) 可知, $(ed)^2 = [e, d]c_1 \in \{b^2, c_1, b^2c_1\}$, 因而 $[e, d] \in \{b^2c_1, 1, b^2\}$. 若 $[e, d] = b^2c_1$, 则对 (i), (ii) 有 $\langle e, bd\rangle \cong \mathrm{D}_8$, 对 (iii) 有 $\langle e, a_1d\rangle \cong \mathrm{D}_8$, 均与 $\mathcal{T}_4$ 群的定义矛盾. 若 $[e, d] = b^2$, 则对 (i)—(iii), 分别有 $\langle a_1e, bd\rangle \cong \mathrm{D}_8$, $\langle e, a_1d\rangle \cong \mathrm{D}_8$ 且 $\langle e, a_1bd\rangle \cong \mathrm{D}_8$, 均与 $\mathcal{T}_4$ 群的定义矛盾. 因而 $[e, d] = 1$, 且 $[e, x] = 1$. 若 $p > 2$, 由 (3) 可得, $\langle x^p, b^p\rangle = \langle b^p, c\rangle$.

断言 4 对 $h\in H$, 有 $[h,x]\in\langle x^p,b^p\rangle=\langle b^p,c_1\rangle$.

由于 $H=\Omega_1(G)\langle b\rangle$, 故可设 $h=gb^l$, 其中 $g\in\Omega_1(G)$ 且 $0\leqslant l\leqslant p-1$. 用 $B_l(g)$ 表示群 $\langle gb^l,x\rangle$. 若 $B_l(g)$ 非交换, 则 $B_l(g)$ 为 p^4 阶内交换群. 由于 $\mho_1(B_l(g))=\langle x^p,b^p\rangle$ 为 p^2 阶初等交换群, 由引理 10.6.1 可知, $B_l(g)\cong \mathrm{M}_p(2,2)$. 若 $[gb^l,x]\neq 1$, 则 $[gb^l,x]\in\Phi(B_l(g))=\mho_1(B_l(g))=\langle x^p,b^p\rangle$. 因而断言 4 对 $h\notin\Omega_1(G)$ 成立. 由于 $[g,x]=[gb,x][b^{-1},x]\in\langle x^p,b^p\rangle$, 故断言 4 对 $h\in\Omega_1(G)$ 成立.

令 $x^p=b^{ip}c_1^j$, 则 $(j,p)=1$. 令 $d=b^{-ij^{-1}}x^{j^{-1}}$, 则可得 $d^p=c_1$. 要证明 $[e,x]=1$, 只需证明 $[e,d]=1$. 由断言 4, 可设 $[e,d]=b^{sp}c_1^t$ 且 $[a_1,d]=b^{up}c_1^v$. 我们可得 $[e,d]=b^{sp}$. (若否, 则 $(t,p)=1$. 由于 $[e,b^sd^t]=(b^{sp}c_1^t)^t=(b^sd^t)^{tp}$, 故 $\langle e,b^sd^t\rangle$ 为 p^3 阶非交换群, 矛盾.)

最后, 我们证明: $[e,d]=1$. 若否, 则 $(s,p)=1$. 若 $(v,p)=1$, 则 $[a_1^se^{-u},d]=c_1^{sv}=d^{svp}$. 因而 $\langle a_1^se^{-u},d\rangle$ 为 p^3 阶内交换群, 矛盾. 若 $[a_1,d]=b^{up}$, 则 $[a_1^se^{1-u},bd]=b^{sp}c_1^s=(bd)^{sp}$. 因此, $\langle a_1^se^{1-u},bd\rangle$ 为 p^3 阶非交换群, 矛盾.

(8) 若否, 由 (2) 可设 $G/H=\langle\bar{x}_1\rangle\times\langle\bar{x}_2\rangle\times\cdots\times\langle\bar{x}_m\rangle$, 其中 $m\geqslant 2$.

若 $p>2$, 则由 (3) 可知, $x_2^p\in\langle x_1^p,b^p\rangle$. 令 $x_2^p=x_1^{sp}b^{tp}$. 则 $(x_2x_1^{-s}b^{-t})^p=1$. 因此 $x_2x_1^{-s}b^{-t}\in\Omega_1(G)\leqslant H$. 因而 $\bar{x}_2=\bar{x}_1^s$, 矛盾.

若 $p=2$, 由 (6), 可设 $G/H=\langle\bar{d_1}\rangle\times\langle\bar{d_2}\rangle\times\cdots\times\langle\bar{d}_m\rangle$, 其中 d_i 满足 (6) 中的 (i), (ii) 或 (iii), 则 $[b,d_1d_2]=1$ 或 b^2, 且 $[a_1b,d_1d_2]=1$ 或 b^2c_1. 由 (4) 可知, $(d_1d_2)^2\in\{b^2,c_1,b^2c_1\}$. 若 $(d_1d_2)^2=b^2$ 且 $[b,d_1d_2]=1$, 则 $(bd_1d_2)^2=1$. 因此 $bd_1d_2\in\Omega_1(G)\leqslant H$. 进而 $\bar{d_1}=\bar{d_2}$, 矛盾. 若 $(d_1d_2)^2=b^2$ 且 $[b,d_1d_2]=b^2$, 则 $\langle b,d_1d_2\rangle\cong \mathrm{Q}_8$, 矛盾. 若 $(d_1d_2)^2=b^2c_1$ 且 $[a_1b,d_1d_2]=1$, 则 $(a_1bd_1d_2)^2=1$. 因此 $a_1bd_1d_2\in\Omega_1(G)\leqslant H$. 进而 $\bar{d_1}=\bar{d_2}$, 矛盾. 若 $(d_1d_2)^2=b^2c_1$ 且 $[a_1b,d_1d_2]=b^2c_1$, 则 $\langle a_1b,d_1d_2\rangle\cong \mathrm{Q}_8$, 矛盾. 若 $(d_1d_2)^2=c_1$, 则 $\langle d_1,d_2\rangle\cong \mathrm{Q}_8$, 矛盾.

(9) 由 (8), 我们可设 $G=H\langle d\rangle$. 令 $L=\langle K,b,d\rangle$. 若 $p=2$, 则由 (6) 可知, d 正规化 $K\rtimes\langle b\rangle$. 若 $p>2$, 则由断言 1 可知, d 也正规化 $K\rtimes\langle b\rangle$. 因此 $|L|=p^5$. 故 L 是引理 10.6.10 中的一个群. 由于 L 中存在两个子群分别同构于 $\mathrm{M}_p(2,2)$ 和 $\mathrm{M}_p(2,1,1)$, 检查可知, L 为引理 10.6.10 中 (2), (4), (5) 或 (6) 型群. 由 (7), $G=L\times E$. 最后, 由定理 10.6.3(7) 可知, $G=L\times E$ 为 $\mathcal{T}_4$ 群. □

10.7 非交换子群的中心均相等的 p 群

群的中心是有限群的一个非常重要的概念. 我们知道, 群 G 为交换群当且仅当 $Z(G)=G$. 由此可以看出, 一个群的中心 $Z(G)$ 的大小在某种意义下可以反映出该群的交换程度. 例如, 利用中心这一概念可以给出幂零群的等价刻画: 有限群 G 为幂零群当且仅当 G 上的中心群列终止于 G. 许多群论学者研究具有某种条件

的中心对有限 p 群结构的影响. 例如, Finogenov 在文献 [64] 中研究了具有循环导群和循环中心的有限 p 群. Janko 在文献 [103] 中研究了只有一个极大子群具有非循环的中心的有限非交换 p 群. 王丽芳等在文献 [227] 中研究 p 群 G 的子群的中心与群 G 的中心的关系对 p 群结构的影响. 特别是在 $p=2$ 的情况下, 分类了非交换子群的中心均相等的非交换 p 群. 而对 $p>2$ 的情况, 则由王丽芳在文献 [231] 中给出了分类. 本节介绍文献 [227] 的工作.

为了方便起见，我们引入以下符号.

$\mathcal{P}$ 群　非交换子群的中心都相等的非内交换的非交换群.

$\mathcal{Q}$ 群　非交换子群均二元生成的 $\mathcal{P}$ 群.

$\mathcal{S}$ 群　至少存在一个非交换子群是非二元生成的 $\mathcal{P}$ 群.

显然, $\mathcal{P}=\mathcal{S}\bigcup\mathcal{Q}$ 且 $\mathcal{S}\bigcap\mathcal{Q}=\varnothing$. 于是, 为了分类 $\mathcal{P}$ 群, 只需分类 $\mathcal{S}$ 群与 $\mathcal{Q}$ 群即可.

首先我们给出两个引理, 它们是简单的但经常被用到.

引理 10.7.1　*若 $G=\langle x,y\rangle$ 是内交换 2 群, 则 $Z(G)=\langle x^2,y^2,[x,y]\rangle$.*

引理 10.7.2　*设 G 为 $\mathcal{P}$ 群. 若 $x,y\in G\backslash Z(G)$ 且 $[x,y]=1$, 则 $C_G(x)=C_G(y)$.*

证明　假设 $C_G(x)\neq C_G(y)$, 不失一般性, 设存在 $z\in C_G(x)\backslash C_G(y)$. 设 $H=\langle x,y,z\rangle$, 则 H 非交换且 $x\in Z(H)=Z(G)$, 与 $x\notin Z(G)$ 矛盾. 故 $C_G(x)=C_G(y)$. □

定理 10.7.3　*设 G 是有限非交换 2 群. 则 G 是 $\mathcal{Q}$ 群当且仅当 G 同构于下列互不同构的群之一.*

(1) $\langle a,b\mid a^{2^c}=b^{2^m}=1,[a,b]=a^{-2}\rangle$, *其中* $m\geqslant 1, c\geqslant 3$;

(2) $\langle a,b\mid a^{2^c}=1,b^{2^m}=a^{2^{c-1}},[a,b]=a^{-2}\rangle$, *其中* $m\geqslant 1, c\geqslant 3$;

(3) $\langle a,b\mid a^{2^c}=b^{2^m}=1,[a,b]=a^{-2+2^{c-1}}\rangle$, *其中* $m\geqslant 1, c\geqslant 3$.

证明　设 G 是 $\mathcal{Q}$ 群, 则对于 G 的任意非交换子群 H, 有 $Z(H)=Z(G)$ 且 $d(H)=2$. 下证 G 有交换极大子群. 若否, 则由定理 8.5.3 可知, G 亚循环. 由定理 6.1.4 可知, G 同构于下列群之一.

(Ⅰ) $G=\langle a,b\mid a^{2^{r+s+u}}=1,b^{2^{r+s+t}}=a^{2^{r+s}},[a,b]=a^{2^r}\rangle$, 其中 r,s,t,u 为非负整数, $r\geqslant 2$ 且 $u\leqslant r$;

(Ⅱ) $G=\langle a,b\mid a^{2^{r+s+v+t'+u}}=1,b^{2^{r+s+t}}=a^{2^{r+s+v+t'}},[a,b]=a^{-2+2^{r+v}}\rangle$, 其中 r,s,v,t,t',u 为非负整数, $r\geqslant 2, t'\leqslant r, u\leqslant 1, tt'=sv=tv=0$, 且若 $t'\geqslant r-1$, 则 $u=0$.

若G为(Ⅰ)型群, 取 $H=\langle a^{2^{s+u-1}},b\rangle$. 若$G$为(Ⅱ)型群, 取 $H=\langle a^{2^{r+s+v+t'+u-2}},b\rangle$, 则 H 为 G 的内交换子群. 由于 $b^2\in Z(H)$ 且 $Z(H)=Z(G)$, 故 $b^2\in Z(G)$. 进而 G 有交换极大子群 $M=\langle a,b^2\rangle$, 矛盾. 因此, G 有交换极大子群.

检查定理 8.4.7 中所列的群, 可得定理中的 3 类群. 再由引理 8.3.2(4) 可知, 它们的非交换子群的中心均相等. □

下面我们分类 $\mathcal{S}$ 群 G. 易见 $|G| \geqslant 2^5$. 分两种情况讨论. 当 G 的阶小于 2^7 时, 用 Magma[37] 检验小群库 [29] 可得所求的群. 因而可设 $\mathcal{S}$ 群 G 的阶不小于 2^7.

引理 10.7.4 设 G 为非交换 2 群且 $|G| \leqslant 2^7$. 则 G 是 $\mathcal{S}$ 群当且仅当 G 同构于下列互不同构的群之一.

(Ⅰ) $|G| = 2^5$.

(Ⅰ-1) SmallGroup$(2^5, 32)$, 其对应的群为

$$\langle a, b, c \mid a^4 = b^4 = c^4 = 1, b^2 = a^2c^2, [b, a] = a^2, [a, c] = c^2, [b, c] = 1\rangle;$$

(Ⅰ-2) SmallGroup$(2^5, 33)$, 其对应的群为

$$\langle a, b, c \mid a^2 = b^4 = c^4 = 1, [a, b] = c^2, [a, c] = b^2c^2, [b, c] = 1\rangle.$$

(Ⅱ) $|G| = 2^6$.

(Ⅱ-1) SmallGroup$(2^6, 64)$, 其对应的群为

$$\langle a, b, c \mid a^4 = b^4 = c^4 = 1, [b, a] = c^2, [c, a] = c^2b^2, [c, b] = 1\rangle;$$

(Ⅱ-2) SmallGroup$(2^6, 82)$, 其对应的群为

$$\langle a, b, c \mid a^4 = b^4 = c^4 = 1, [b, a] = c^2, [c, a] = c^2b^2, [c, b] = b^2a^2,$$
$$[a^2, b] = [a^2, c] = [b^2, a] = [b^2, c] = [c^2, a] = [c^2, b] = 1\rangle;$$

(Ⅱ-3) SmallGroup$(2^6, 113)$, 其对应的群为

$$\langle a, b, c \mid a^8 = b^4 = c^4 = 1, b^2 = c^2, [a, b] = b^2, [c, a] = a^4, [c, b] = 1\rangle;$$

(Ⅱ-4) SmallGroup$(2^6, 180)$, 其对应的群为

$$\langle a, b, c \mid a^4 = b^4 = c^8 = 1, b^2 = a^2c^4, [b, a] = a^2, [a, c] = c^2, [c, b] = 1\rangle;$$

(Ⅱ-5) SmallGroup$(2^6, 245)$, 其对应的群为

$$\langle a, b, c, d \mid a^4 = b^4 = c^4 = d^4 = 1, a^2 = d^2, b^2 = c^2, [b, a] = a^2, [c, a] = c^2,$$
$$[c, b] = [d, a] = a^2b^2, [d, b] = a^2, [d, c] = 1\rangle.$$

(Ⅲ) $|G| = 2^7$.

(Ⅲ-1) SmallGroup$(2^7, 300)$, 其对应的群为

$$\langle a, b, c \mid a^8 = b^8 = c^4 = 1, b^4 = c^2, [a, b] = b^2, [c, a] = a^4, [c, b] = 1\rangle;$$

(Ⅲ-2) SmallGroup(2^7, 571), 其对应的群为

$$\langle a,b,c \mid a^8=b^4=c^4=1,[b,a]=c^2,[c,a]=c^2b^2,[c,b]=1\rangle;$$

(Ⅲ-3) SmallGroup(2^7, 895), 其对应的群为

$$\langle a,b,c \mid a^{16}=b^4=c^4=1,b^2=c^2,[a,b]=b^2,[c,a]=a^8,[c,b]=1\rangle;$$

(Ⅲ-4) SmallGroup(2^7, 985), 其对应的群为

$$\langle a,b,c \mid a^4=b^4=c^{16}=1,b^2=a^2c^8,[b,a]=a^2,[a,c]=c^2,[c,b]=1\rangle.$$

SmallGroup (o,n) 表示小群库中 o 阶群中第 n 个群.

定理 10.7.5 设 G 是有限非交换 2 群且 $|G|\geqslant 2^7$. 则 G 是 $\mathcal{S}$ 群当且仅当 G 同构于下列互不同构的群之一.

(1) $G=\langle a,b,c \mid a^{2^n}=b^4=c^4=1,[b,a]=c^2,[c,a]=c^2b^2,[c,b]=1\rangle, n\geqslant 3$;

(2) $G=\langle a,b,c \mid a^4=b^4=c^{2^n}=1,b^2=a^2c^{2^{n-1}},[b,a]=a^2,[a,c]=c^2,[c,b]=1\rangle$, 其中 $n\geqslant 4$;

(3) $G=\langle a,b,c \mid a^{2^m}=b^{2^n}=c^4=1,b^{2^{n-1}}=c^2,[a,b]=b^2,[c,a]=a^{2^{m-1}},[c,b]=1\rangle$, 其中 $m\geqslant 3, n\geqslant 2$.

证明 设 G 是 $\mathcal{S}$ 群, 下面分两种情形讨论.

情形 1 G 的每个非交换真子群 H 均二元生成.

由于 $|G|\geqslant 2^7$, 由定理 8.6.2, 可设 G 有交换极大子群. 由于 G 是 $\mathcal{S}$ 群, 故 $d(G)=3$. 由定理 8.6.1 可得, G 是 $\mathcal{A}_2$ 群. 由于 $d(G)=3$ 且 G 有交换极大子群, 故 G 为定理 9.3.1 所列的群. 检查该定理可得, G 为 (1) 型群, 或 $n=2$ 的 (3) 型群.

情形 2 存在 G 的非交换子群 H 使得 $d(H)\geqslant 3$.

若 $|G|=2^7$, 由引理 10.7.4 可知, 结论成立. 下设 $|G|\geqslant 2^8$.

设 M 为 G 的极大子群使得 $H\leqslant M$, 则 M 是 $\mathcal{S}$ 群. 由归纳假设, M 同构于定理中所列的群之一.

子情形 2.1 $M=\langle a,b,c \mid a^{2^n}=b^4=c^4=1,[b,a]=c^2,[c,a]=c^2b^2,[c,b]=1\rangle$, 其中 $n\geqslant 1$.

显然 $Z(M)=\langle a^2,b^2,c^2\rangle$ 且 M 有唯一的极大子群 $A=\langle a^2,b,c\rangle$. 因而 $A\trianglelefteq G$. 由于 $|G/A|=4$, 故 $G'\leqslant A$. 由题设可知, $Z(G)=Z(M)=\langle a^2,b^2,c^2\rangle$. 取 $x\in G\backslash M$, 则 $G=\langle x,a,b,c\rangle$.

设 $[a,x]=a^{2s}b^tc^u$. 由

$$1=[a^2,x]=[a,x]^2[a,x,a]=a^{4s}b^{2(t+u)}c^{2t}$$

可得, $2^{n-2}|s$, $2|t$ 且 $2|u$. 因而 $[a,x]=a^{2^{n-1}i_1}b^{2j_1}c^{2k_1}$. 由 $[a,b]=c^2$ 和 $[a,c]=b^2c^2$ 可得, $[a,xc^{j_1}b^{j_1+k_1}]=a^{2^{n-1}i_1}$. 用 $xc^{j_1}b^{j_1+k_1}$ 替换 x, 可设 $[a,x]=a^{2^{n-1}i_1}$. 若 $[a,x]\neq 1$, 则由定理 1.7.7 可知, $\langle a,x\rangle$ 内交换. 由引理 10.7.1 可得

$$Z(\langle a,x\rangle)=\langle a^2,x^2\rangle\neq\langle a^2,b^2,c^2\rangle=Z(G),$$

矛盾. 因而 $[a,x]=1$.

设 $[b,x]=a^{2s}b^tc^u$. 由 $1=[b^2,x]=[b,x]^2=a^{4s}b^{2t}c^{2u}$ 可得, $2^{n-2}|s$, $2|t$ 且 $2|u$. 因此, 可设 $[b,x]=a^{2^{n-1}i_2}b^{2j_2}c^{2k_2}$. 同理, $[c,x]=a^{2^{n-1}i_3}b^{2j_3}c^{2k_3}$. 因而 $[b,x],[c,x]\in Z(G)$. 故 $G'\leqslant Z(G)$ 且 $\exp G'=2$.

若 $G/A\cong \mathrm{C}_4$, 则 $G/A=\langle xA\rangle$ 且 $M/A=\langle aA\rangle=\langle x^2A\rangle$. 因而 $x^2a^{-1}\in A$. 设 $x^2=aa'$, 其中 $a'\in A$, 则

$$1=[b,x]^2=[b,x^2]=[b,aa']=[b,a]=c^2,$$

矛盾. 因而 $G/A\cong \mathrm{C}_2\times\mathrm{C}_2$ 且 $x^2\in A$.

由于 $[a,x]=1$, 故可设 $x^2=b^tc^u$. 由

$$1=[a,x]^2=[a,x^2]=b^{2u}c^{2(t+u)}$$

可得, $2|t$ 且 $2|u$. 设 $x^2=b^{2j}c^{2k}$.

由于 $x\notin Z(G)$, 由引理10.7.2可得

$$[b,x]=a^{2^{n-1}i_2}b^{2j_2}c^{2k_2}\neq 1,\quad [c,x]=a^{2^{n-1}i_3}b^{2j_3}c^{2k_3}\neq 1,$$

且

$$[bc,x]=a^{2^{n-1}(i_2+i_3)}b^{2(j_2+j_3)}c^{2(k_2+k_3)}\neq 1.$$

易见 $\{i_2,i_3,i_2+i_3\}$ 中至少有一个是偶数. 不失一般性, 设 i_2 为偶数, 则由引理 10.7.1 可知, $Z(\langle b,x\rangle)\leqslant\langle b^2,c^2\rangle$. 由于 G 为 $\mathcal{P}$ 群, 故 $Z(G)=Z(\langle b,x\rangle)$. 因此, $a^2=1$ 且 $n=1$.

用 xa^{k_2} 替换 x, 则 $[a,x]=1$ 且 $[b,x]=b^{2j_2}\neq 1$. 因而 $[b,x]=b^2$. 由引理 1.7.7 可知, $\langle b,x\rangle$ 内交换. 再由引理 10.7.1 可得, $x^2=b^{2j}c^2$.

由引理 10.7.2 可知, $C_G(b)=C_G(c)=C_G(bc)$. 因而, $[c,x]\neq[b,x]=b^2$. 由于 $[c,ax]\neq 1$, 故 $[c,x]\neq[c,a]=b^2c^2$ 且 $[c,x]=c^2$. 由定理 1.7.7 可得, $\langle c,x\rangle$ 内交换. 再由引理 10.7.1 可得, $Z(\langle c,x\rangle)=Z(G)=\langle c^2,x^2\rangle$. 因而 $x^2=b^2c^2$. 由于 $[bc,x]=[b,x][c,x]=b^2c^2$, 故 $Z(\langle bc,x\rangle)=\langle b^2c^2\rangle\neq Z(G)=\langle b^2,c^2\rangle$, 矛盾.

子情形 2.2 $M=\langle a,b,c\mid a^4=b^4=c^{2^n}=1,b^2=a^2c^{2^{n-1}},[b,a]=a^2,[a,c]=c^2,[c,b]=1\rangle$, 其中 $n\geqslant 3$.

显然 $Z(M)=\langle a^2,b^2\rangle$ 且 M 有唯一的交换极大子群 $A=\langle b,c\rangle$. 因而 $A\trianglelefteq G$. 由于 $|G/A|=4$, 故 $G'\leqslant A$. 由假设可知, $Z(G)=Z(M)=\langle a^2,b^2\rangle$. 取 $x\in G\backslash M$, 则 $G=\langle x,a,b,c\rangle$.

设 $[b,x]=b^sc^t$, 由于

$$1=[b^2,x]=[b,x]^2=b^{2s}c^{2t},$$

故 $2|s$ 且 $2^{n-1}|t$. 因而可设 $[b,x]=b^{2i_2}c^{2^{n-1}j_2}$.

设 $[c,x]=b^sc^t$, 由

$$1=[c^{2^{n-1}},x]=c^{2^{n-1}t},\quad 1=[x,a,c][a,c,x][c,x,a]=[c^2,x][b^sc^t]=b^{2s}a^{2s}$$

可知, $2|t$ 且 $2|s$. 故可设 $[c,x]=b^{2i_3}c^{2t'}$.

假设 $G/A\cong \mathrm{C}_4$, 则 $G/A=\langle xA\rangle$ 且 $M/A=\langle aA\rangle=\langle x^2A\rangle$. 进而可知, $x^2a^{-1}\in A$. 设 $x^2=ab^sc^t$, 则

$$1=[b,x]^2=[b,x^2]=[b,ab^sc^t]=[b,a]=a^2,$$

矛盾. 因而 $G/A\cong \mathrm{C}_2\times\mathrm{C}_2$ 且 $x^2\in A$.

由 $1=[c,x^2]=[c,x]^2[c,x,x]=c^{4t'}[b^{2i_3}c^{2t'},x]=c^{4t'+4t'^2}$ 可得, $2^{n-2}|t'(t'+1)$. 由此可得, $2^{n-2}|t'$ 或 $2^{n-2}|t'+1$. 因而

$$[c,x]=b^{2i_3}c^{2^{n-1}j_3}\quad 或\quad [c,x]=b^{2i_3}c^{2^{n-1}j_3-2}.$$

若 $[c,x]=b^{2i_3}c^{2^{n-1}j_3-2}$, 则 $[c,xa]=[c,a][c,x][c,x,a]=b^{2i_3}c^{2^{n-1}j_3}$. 用 xa 替换 x, $[c,x]=b^{2i_3}c^{2^{n-1}j_3}$.

若 $[c,x]=b^{2i_3}c^{2^{n-1}j_3}\neq 1$, 则 $\langle c,x\rangle$ 内交换, 且 $c^2\in Z(\langle c,x\rangle)$. 由假设可知, $c^2\in Z(G)$, 矛盾. 因而 $[c,x]=1$. 由引理 10.7.2 可得, $[b,x]=1$.

设 $[a,x]=b^sc^t$, 由于

$$1=[a^2,x]=[a,x]^2[a,x,a]=b^{2s}a^{2s},$$

故 $2|s$. 因而 $[a,x]=b^{2i_1}c^t$. 由于 $[a,xb^{i_1}]=c^{t+i_12^{n-1}}$, 用 xb^{i_1} 替换 x, 可设 $[a,x]=c^{j_1}$.

若 $2|j_1$, 则 $j_1=2j_1'$. 由于

$$[a,xc^{-j_1'}]=[a,x][a,c^{-j_1'}]=c^{2j_1'}c^{-2j_1'}=1,$$

故 $xc^{-j_1'}\in Z(G)\leqslant A$, 进而 $x\in A$, 矛盾. 因此 $2\nmid j_1$. 故可设 $[a,x]=c$.

设 $x^2=b^sc^t$, 则 $[a,x^2]=[a,x]^2[a,x,x]=c^2$. 另一方面, $[a,x^2]=[a,b^sc^t]=a^{2s}c^{2t}$. 因此 $2|s$ 且 $2^{n-1}|1-t$. 设 $x^2=b^{2i}c^{1-2^{n-1}k}$.

设 $H=\langle xbac, c^{2^{n-2}}\rangle$, 由于 $[xbac, c^{2^{n-2}}]=[a,c^{2^{n-2}}]=c^{2^{n-1}}$, 由定理 1.7.7 可得, H 为内交换群. 由引理 10.7.1 可知,

$$Z(H)=\langle (xbac)^2, c^{2^{n-1}}, [xbac, c]\rangle.$$

由于

$$(xbac)^2=b^{2(i+1)} \quad 且 \quad Z(H)=Z(G)=\langle b^2, c^{2^{n-1}}\rangle,$$

故 $2|i$ 且 $x^2=c^{1-2^{n-1}k}=ca^{2k}b^{2k}=[a,x]a^{2k}b^{2k}$.

由于 $[a,xb^k]=x^2b^{2k}=(xb^k)^2$, 用 xb^k 替换 x, 可设 $[a,x]=x^2$. 因此

$$G=\langle a,b,x | a^4=b^4=x^{2^{n+1}}=1, b^2=a^2x^{2^n}, [b,a]=a^2, [a,x]=x^2, [b,x]=1\rangle.$$

子情形 2.3 $M=\langle a,b,c \mid a^{2^m}=b^{2^n}=c^4=1, b^{2^{n-1}}=c^2, [a,b]=b^2, [c,a]=a^{2^{m-1}}, [c,b]=1\rangle$, 其中 $m\geqslant 3, n\geqslant 2$.

同子情形 2.2 的证明可得, 在这种情形下, G 为 (3) 型群.

比较三个群的中心的生成元以及中心的阶可知, 定理中的群是互不同构的.

下面证明群 (1)—(3) 为 $\mathcal{S}$ 群.

设 G 为 (1) 型群, 由于 G 是 $\mathcal{A}_2$ 群, 故 G 的每个非交换子群 M 为 G 的极大子群. 由于 $Z(G)=\langle a^2,b^2,c^2\rangle=\Phi(G)$, 故 $Z(G)\leqslant M$. 再由 $|M:Z(G)|=2^2$ 可知, $Z(G)=Z(M)$. 因此 G 为 $\mathcal{S}$ 群.

设 G 为 (2) 型群, 则 $\Omega_1(G)=Z(G)=\langle a^2,b^2\rangle$ 且 $M=\langle a^2,b,c\rangle=\langle b,c\rangle$ 为 G 的唯一交换极大子群. 设 H 为 G 的非交换子群. 则 $G=HM$ 且存在 $h\in H$ 使得 $h\notin M$. 因此, $G=\langle h\rangle M$ 且 $H=\langle h\rangle(H\bigcap M)$. 下面证明 $Z(H)=Z(G)$.

由于 $H=\langle h\rangle(H\bigcap M)$ 非交换, 故存在 $h'\in H\bigcap M$ 使得 $[h,h']\neq 1$. 设 $h=ab^ic^j$, $h'=b^{i'}c^{j'}$, 则 $[h,h']=b^{2i'}c^{2^{n-1}i'+2j'}=h'^2c^{2^{n-1}i'}\neq 1$.

若 $2\nmid i'$, 则 $c^{2^{n-1}}=h'^{-2}[h,h']\in H$. 若 $2|i'$, 由 $h'\notin Z(G)=\Omega_1(G)$ 可知, $h'^2=c^{2j'}\neq 1$. 因而 $c^{2^{n-1}}\in H$.

由于 $h^2=b^2c^{2^{n-1}(i+1)}$, 故 $b^2=h^2c^{2^{n-1}(i+1)}\in H$. 因此 $Z(G)=\Omega_1(G)\leqslant H$.

另一方面, 由于 $H\bigcap M$ 为 H 的交换极大子群, 故 $Z(H)\leqslant H\bigcap M$. 由 $G=HM$ 及 M 交换可知, $Z(H)\leqslant Z(G)$. 所以 $Z(G)=Z(H)$, 即 G 为 $\mathcal{S}$ 群.

设 G 为 (3) 型群. 若 $n=2$, 则 G 为 $\mathcal{A}_2$ 群. 因而, G 的每个非交换子群 M 为 G 的极大子群. 由于 $Z(G)=\langle a^2,b^2\rangle=\Phi(G)$, 故 $Z(G)\leqslant M$. 再由 $|M:Z(G)|=2^2$ 可知, $Z(G)=Z(M)$. 因此 G 为 $\mathcal{S}$ 群.

若 $n > 2$, 则 $Z(G) = \langle a^2, c^2 \rangle$ 且 $M = \langle a^2, b, c \rangle$ 为 G 的交换极大子群. 设 H 为 G 的非交换子群, 则 $G = HM$ 且存在 $h \in H$ 使得 $h \notin M$. 因而, $G = \langle h \rangle M$ 且 $H = \langle h \rangle (H \bigcap M)$. 由于 $H' \neq 1$, 故存在 $h' \in H \bigcap M$ 使得 $[h, h'] \neq 1$. 设 $h = ab^j c^k$, $h' = a^{2i'} b^{j'} c^{k'}$, 则

$$h^2 = a^{2+2^{m-1}k} c^{2k}, \quad h'^2 = a^{4i'} b^{2j'} c^{2k'}, \quad [h, h'] = b^{2j'} a^{2^{m-1}k'} \neq 1.$$

由于 $h^2 = a^{2+2^{m-1}k} c^{2k}$, 故 $a^4 \in H$. 因而 $b^{2j'}, c^{2k'} \in H$. 由 $[h, h'] = b^{2j'} a^{2^{m-1}k'} \neq 1$ 可得, $2^{n-1} \nmid j'$ 或 $2 \nmid k'$. 因而 $c^2 \in H$. 由 $h^2 = a^{2+2^{m-1}k} c^{2k}$ 可知, $a^2 \in H$. 因此 $Z(G) \leqslant H$.

另一方面, 由于 $H \bigcap M$ 为 H 的交换极大子群, 故 $Z(H) \leqslant H \bigcap M$. 由 $G = HM$ 及 M 交换可知, $Z(H) \leqslant Z(G)$. 所以 $Z(G) = Z(H)$, 即 G 为 $\mathcal{S}$ 群. □

第 11 章　正规性较强的有限 p 群

众所周知, 正规子群在有限群的研究中起着极其重要的作用. 早在 1897 年, Dedekind[57] 确定了所有子群都正规的有限群, 这样的群被称为 Dedekind 群. 非交换的 Dedekind 群称为 Hamilton 群. 1933 年, Baer 在文献 [14] 中对于无限 Dedekind 群给出了分类. 自那时以来, 许多群论学家开始研究与 Dedekind 群的结构接近的群类, 获得了丰富的成果. 例如, 弱化子群的正规性条件, 许多子群概念被提出. 最常见的有拟正规子群、s 拟正规子群、共轭置换子群、次正规子群、半正规子群、s 半正规子群、c 正规子群、TI 子群等, 每个子群均为拟正规子群 (或者上述提到的其他类型的子群) 的有限群的结构分别被研究和确定, 见文献 [67], [131], [194], [220], [226], [245], [269]. 从 "次正规长度" 的角度研究比 Dedekind 群更广的有限群也有许多结果. 次正规子群 H 到 G 的最短的次正规群列的长度称为 H 的次正规长度. 群 G 的所有次正规子群的次正规长度的最大值称为 G 的次正规长度. 显然, 次正规长度为 1 的群是 Dedekind 群, 许多学者研究次正规长度为 2 的群, 见文献 [145], [146], [175], [178]—[180].

另外, 也有一些学者对非正规子群的正规化子和正规闭包施加某种限制来研究有限群, 例如, Mann 在文献 [148] 确定了非正规子群的正规化子均是极大子群的有限非可解群. 吕恒等在文献 [138], [139] 确定了非正规子群的正规闭包较小的有限 p 群. 郭秀云、张军强等分别在文献 [261], [284] 研究了非正规子群的正规闭包较大的有限 p 群. 王丽芳等在文献 [228] 分类了非正规子群的正规闭包同阶的有限 p 群. 余大鹏等在文献 [251] 分类了非正规子群的正规闭包均内交换的有限 p 群. 另一方面, 黎先华、张军强、张勤海、张小红等在文献 [134], [262], [277], [281] 等分别研究了非正规子群的正规化子较小的有限 p 群.

Cappitt 等从非正规子群生成真子群的角度研究广义的 Dedekind 群, 见文献 [45], [110], [191], [189]. 从某些特殊的子群出发, 研究与 Dedekind 群的结构相近的有限群也有许多结果, 见文献 [32], [45], [73], [110], [147], [189], [191].

由于有限 p 群存在可能阶的正规子群, Passman 在文献 [181] 研究 p 群的非正规子群. 这是一篇重要的 p 群论文. 该文分类了非正规子群均为 p 阶的 p 群, 更一般地, 除了某些小阶群之外, 分类了非正规子群均循环的 p 群. 在某种意义上, Passman 研究的是具有 "很多" 正规子群的 p 群. 继 Passman 的结果之后, 张丽华等[263] 分类了非正规交换子群均循环的 p 群. Zappa[253, 254]、张军强 [259] 先后独

立地分类了非正规子群均同阶的 p 群. 张勤海等在文献 [275], [278], [279] 先后分类了非正规子群的阶分别不超过 p^2 和 p^3 的 p 群.

还有某些学者从非正规子群的共轭类数出发, 研究比 Dedekind 群更大的群类结构, 令 $\nu(G)$ 表示群 G 的非正规子群的共轭类数. 显然, $\nu(G)=0$ 的群 G 恰为 Dedekind 群. $\nu(G)\leqslant 2$ 的有限群 G 的结构分别被 Brandl, Mousavi, 陈贵云等所确定, 见文献 [40], [47], [163]. 对于有限 p 群而言, La Haye 和 Rhemtulla[117] 证明了: 若 $\nu(G)>1$, 则 $\nu(G)\geqslant p$. 对于 $p=2$, $\nu(G)\leqslant 3$ 的有限 2 群 G 分别被 Schmidit, Mousavi 所分类, 见文献 [164], [199], [200]. 对于 $p\neq 2$, Fernández-Alcober 和 Legarreta[62] 分类了 $\nu(G)=p$ 的有限 p 群. Brandl[42] 分类了 $\nu(G)=p+1$ 的有限 p 群. 曲海鹏[123] 研究 $\nu(G)$ 可能取到的值, 分类了比文献 [42], [62] 更广的一类 p 群. 本章主要介绍比 Dedekind p 群更广的某些 p 群类的分类结果.

11.1 非正规子群均循环的 p 群

Passman 在文献 [181] 中研究了 p 群的非正规子群, 并且给出了非正规子群均循环的有限 p 群的分类.

称 $H_1>H_2>\cdots>H_k$ 为 G 的非正规子群链, 若 $H_i\ntrianglelefteq G$ 且 $|H_i:H_{i+1}|=p$, 其中 $i=1,2,\cdots,k$, 并且这个非正规子群链的长度为 k. 记 $\mathrm{chn}(G)$ 为 G 的非正规子群链的最大长度.

设 G 为有限 p 群, H 为 G 的非正规子群. 称 H 为 G 的极大非正规子群, 如果对每个满足 $K>H$ 的子群 K, 有 $K\trianglelefteq G$; 而称 H 为 G 的极小非正规子群, 如果对每个满足 $K<H$ 的子群 K, 有 $K\trianglelefteq G$.

引理 11.1.1 ([181] 中的引理 1.4) *设 H 是有限 p 群 G 的极小非正规子群. 则 H 循环.*

引理 11.1.2 ([181] 中的引理 2.1) *设 G 是有限非 Dedekind p 群. 则存在 G 的正规子群 $K\lessdot G'$ 使得 G/K 不是 Dedekind 群.*

引理 11.1.3 *设 G 为有限 p 群. 则 $\mathrm{chn}(G)=1$ 当且仅当 G 的所有非正规子群均循环.*

证明 设 $\mathrm{chn}(G)=1$. 任取 $H\ntrianglelefteq G$, 则 H 为 G 的极小非正规子群. 由引理 11.1.1 可知, H 循环. 反之, 设 G 非 Dedekind 群且 G 的所有非正规子群均循环. 任取 $H\ntriangleleft G$, 则 H 循环. 令 K 为 G 的包含 H 的极大循环子群并且选取 G 的适当子群 L 使得 $|L:K|=p$. 则 $L\lhd G$. 由于 L 二元生成, 因此 $\Phi(K)=\Phi(L)\lhd G$. 从而 $H=K$. 故 H 为 G 的极大非正规子群且 $\mathrm{chn}(G)=1$. □

定理 11.1.4 *设 G 为有限 p 群. 若 $\mathrm{chn}(G)=1$, 则 G 为以下群之一.*

(i) $\mathrm{M}_p(n,m)$, *其中 $n\geqslant 2$, $m\geqslant 1$.*

(ii) $G = \mathrm{C}_{2^n} * G_0$, 其中 $n \geqslant 2$, 并且若 $p = 2$, 则 $G_0 = \mathrm{D}_8$; 若 $p > 2$, 则 $G_0 = \mathrm{M}_p(2,1)$ 或 $\mathrm{M}_p(1,1,1)$.

(iii) $G = \mathrm{C}_{2^n} \times \mathrm{Q}_8$, 其中 $n \geqslant 2$.

(iv) 阶 $\leqslant 2^7$ 的 2 群中的某些群.

(v) 3^4 阶非正则的某些群.

证明 以下总假设, 当 $p=2$ 时, $|G| \geqslant 2^8$. 注意到 G 非交换. 若 G 无 (p,p) 型交换正规子群, 则 $p=2$ 且 G 为极大类 2 群. 因为 $\mathrm{chn}(G)=1$, 由 [181] 中的引理 2.6 可知, $2^3 \leqslant |G| \leqslant 2^4$, 矛盾. 从而 G 中必定存在 (p,p) 型交换正规子群 W. 再由 [181] 中的引理 2.5 可知, $\mathrm{chn}(G/W)=0$. 故 G/W 为 Dedekind 群. 若 G/W 非交换, 则由 [181] 中的定理 1.8.1 可知, $G/W = \overline{Q} \times \overline{A}$, 其中 $\overline{A}$ 为初等交换群, $\overline{Q} \cong \mathrm{Q}_8$. 又由 [181] 中的定理 2.8 可知, G 至多四元生成. 因此 $|G/W| \leqslant 2^5$. 故 $|G| \leqslant 2^7$, 矛盾. 因此 G/W 交换. 从而 $G' \leqslant W$ 且 $G' \cong \mathrm{C}_p$ 或者 $\mathrm{C}_p \times \mathrm{C}_p$. 当然, 这个结论对于 G 的所有 (p,p) 型交换子群 W 均成立. 接下来, 断言 G 无 (p,p,p) 型交换子群. 若否, 可选取 W 为其任意极大子群, 则 G' 包含在所有这些极大子群中. 从而 $G'=1$, 即 G 交换, 矛盾. 下面分 $Z(G)$ 循环和非循环两种情形来讨论.

情形 1 $Z(G)$ 循环.

令 $Z = \Omega_1(Z(G))$, 则 $|Z| = p$. 任取 J 为 G 的另一个 p 阶子群, 则 $J \ntrianglelefteq G$ 且 $W = Z \times J$ 为 G 的一个 (p,p) 型交换正规子群. 令 $N = N_G(J)$. 由 [181] 中的引理 1.3 可知, $|G:N| = p$ 且 N/J 或循环或为广义四元数群. 显然 $1 = \mathrm{chn}(G) \geqslant \mathrm{chn}(N) \geqslant \mathrm{chn}(N/J)$. 若 N/J 为广义四元数群, 由 [181] 中的引理 2.6 可知 $|N:J| \leqslant 2^4$. 从而 $|G| \leqslant 2^6$, 矛盾. 故 N/J 循环且 N 交换. 由于 $W \leqslant N$, 因此 N 非循环. 故可设 $N = A \times J$, 其中 A 循环. 令 $G = \langle N, u\rangle$. 由于 N 交换, 因此映射 $y \longmapsto y^{-1}y^u$ 为 N 到 G' 的同态满射且核为 $Z(G)$. 从而 $N/Z(G) \cong G'$.

若存在 $x \in G \backslash N$ 且 $o(x) = p$, 则 $\langle Z, x\rangle$ 为 G 的 (p,p) 型交换子群. 从而 $\langle Z, x\rangle \lhd G$. 进而 $G' \leqslant \langle Z, J\rangle \bigcap \langle Z, x\rangle = Z$. 因此 $|G'| = p$. 又因为 $N/Z(G) \cong G'$, 所以 $|N:Z(G)| = p$. 故 $J \nleqslant Z(G)$. 因而 $N = Z(G) \times J$. 由 $\langle W, x\rangle = G_0$ 为 p^3 阶非交换群且 $G = Z(G)G_0$, 可得定理中的群 (ii).

下面假设 $G \backslash N$ 中不存在 p 阶元 x. 考虑商群 G/W. 若 G/W 循环, 注意到 G 的所有阶 $\geqslant p^2$ 的子群交 $Z(G)$ 均不为 1, 则 G 亚循环. 进一步, 由于 $G' \leqslant W$ 且 G' 循环, 因此可得定理中的群 (i).

设 G/W 非循环. 由于 G/W 交换, 不妨设 G/W 为 (p^a, p) 型交换群, 其中 $a \geqslant 1$. 令 $G \geqslant R > W$ 且 R/W 为 (p,p) 型交换群. 若 $p=2$, 令 $x \in R \backslash (R \bigcap N)$. 则 $x \notin \mathrm{C}_G(J)$. 从而 $\langle W, x\rangle \cong \mathrm{D}_8$. 注意到 $\langle W, x\rangle$ 有 5 个对合. 因此存在 2 阶元 $y \in \langle W, x\rangle \backslash W \subseteq G \backslash N$, 矛盾. 因此 $p > 2$. 断言: 映射 $x \longmapsto x^p$ 不是 R 的同态映射. 若否, 由于 $\Omega_1(R) = W$, 因此 W 中的每个元素均为 p 次幂的形式. 特别地, 存

在 $x \in R$ 使得 $\langle x^p \rangle = J$ 且 $\langle x \rangle > \langle x^p \rangle$ 为 G 的长为 2 的非正规子群链, 矛盾. 由 $R' \leqslant G'$ 可得 R' 初等交换且 R 非正则. 又因为 $|R| = p^4$, 所以 $p = 3$ 且 $c(R) = 3$. 由于 $N/Z(G)$ 初等交换且 $R \bigcap N$ 为 (p^2, p) 型交换群, 因此若 $a \geqslant 2$, 则 $R \bigcap N$ 包含一个 p^2 阶中心元且 $|R : Z(R)| \leqslant p^2$, 矛盾. 故 $a = 1$ 且 $G = R$, 即可得定理中的群 (v).

情形 2　$Z(G)$ 非循环.

令 $Z = Z(G)$ 且 $W = \Omega_1(Z)$. 因为 G 无 (p,p,p) 型交换子群, 所以 $W = \Omega_1(G)$ 为 (p,p) 型的. 又因为 $G' \leqslant W$, 所以 $c(G) = 2$. 进而, 由 [181] 中的引理 1.5 可知, G/Z 初等交换. 不妨设 $p > 2$ 或 $p = 2$ 且 $\{x \mid x^2 \in G'\} \leqslant Z$. 下证在此假设下, 映射 $x \longmapsto x^p$ 为 G/W 到 Z 的一一映射. 显然, 若 $p > 2$, 则 G 正则. 故映射 $x \longmapsto x^p$ 为核等于 $\Omega_1(G)$ 的同态映射. 设 $p = 2$. 若 $x^2 = y^2$, 则 $(xy^{-1})^2 = x^2[x,y]y^{-2} = [x,y]$. 由假设知, $xy^{-1} \in Z$. 故 x, y 可交换且 $xy^{-1} \in W = \Omega_1(G)$. 因此 $|Z| \geqslant |G/W|$. 又注意到 G 非交换. 因此 G/Z 为 (p,p) 型交换群并且映射 $x \longmapsto x^p$ 为到 Z 的满射. 接下来, 由 [181] 中的引理 1.5 可知, $|G'| = p$. 因此可选取 $u, v \in Z$ 使得 $Z = \langle u \rangle \times \langle v \rangle$ 且 $G' \leqslant \langle u \rangle$. 若存在 $x, y \in G$ 使得 $x^p = u$, $y^p = v$, 则 $\langle x \rangle \lhd G$ 且 $G = \langle x, y \rangle$. 从而亦可得定理中的群 (i).

以下总假设 $p = 2$ 且 $\{x \mid x^2 \in G'\} \not\leqslant Z$. 令 $x \in G \backslash Z$ 且 $x^2 \in G'$. 由于 $\Omega_1(G) \leqslant Z$, 因此 $|\langle x \rangle| = 4$. 若存在 $y \in Z$ 使得 $y^2 = x^2$. 则 $(xy^{-1})^2 = 1$. 因此 $xy^{-1} \in W \leqslant Z$. 故 $x \in Z$, 矛盾. 因此可设 $Z = Z_1 \times \langle x^2 \rangle$, 其中 Z_1 循环. 因为 $\Omega_1(G) \leqslant Z$ 且 $\Omega_2(G) \not\leqslant Z$, 由 [181] 中的命题 1.6 知, G 中存在 4 阶非正规子群 H. 进一步, 由 [181] 中的引理 1.3 和引理 1.4 知, H 循环, $|G/N_G(H)| = 2$ 且 $N_G(H)/H$ 循环或者为广义四元数群. 若 $N_G(H)/H$ 为广义四元数群, 注意到 G' 初等交换. 则 $|N_G(H)/H| = 8$ 且 $|P| = 2^6$, 矛盾. 故 $N_G(H)/H$ 循环且 $d(G) \leqslant 3$.

若 $|G'| = 2$, 则 G/Z 必有偶数个生成元. 又因为 G/Z 初等交换, 所以 $|G/Z| = 4$. 由于 $x^2 \in G'$, 因此 $\langle x \rangle \geqslant G'$. 从而 $\langle x \rangle \lhd G$. 于是 $Z_1 \bigcap \langle x \rangle = 1$. 进而, $\overline{Z}_1 = Z_1\langle x \rangle/\langle x \rangle$ 在 $G/\langle x \rangle$ 中指数为 2. 若 $G/\langle x \rangle$ 循环, 则 G 同构于定理中的群 (i). 若 $G/\langle x \rangle$ 非循环, 则可设 $G/\langle x \rangle = \overline{Z}_1 \times \overline{B}$, 其中 $|\overline{B}| = 2$. 令 $G \geqslant B \geqslant \langle x \rangle$ 且 $B/\langle x \rangle = \overline{B}$. 则 $Z_1 B = G$ 且 $Z_1 \bigcap B = Z_1 \bigcap \langle x \rangle \bigcap B = 1$. 故 $G = Z_1 \times B$. 进一步, 由于 G 非交换且 $\Omega_1(B) = \langle x^2 \rangle$. 所以 $B \cong Q_8$, 即可得 P 为定理中的群 (iii).

若 $|G'| = 4$, 则 $G' = W$. 显然 $|G : Z| \not\leqslant 4$. 进而可证 $|G : Z| = 2^3$ 且 $Z = \Phi(G)$. 令 $1 < J < G'$. 则 $J \lhd G$. 故 $|(G/J)'| = 2$. 由于 G/J 至多三元生成, 因此 $|G/J : Z(G/J)| = 4$. 从而存在 $y \in G \backslash Z(G)$ 使得 $[G, y] \subseteq J$ 且 $|G : C_G(y)| = 2$. 又由 $|C_G(y) : \langle y, Z \rangle| = 2$, 故 $A = C_G(y)$ 为 P 的指数为 2 的交换正规子群. 由于 $\Omega_1(A) \leqslant Z$ 且 A/Z 初等交换, 因此可令 $A = \langle u \rangle \times \langle v \rangle$ 为 $(2^n, 4)$ 型交换群, 其中 $|\langle u \rangle| = 2^n$, $|\langle v \rangle| = 4$. 因为 $|G| \geqslant 2^8$, 所以 $n \geqslant 3$. 由于 $|G/\Phi(G)| = 2^3$, 因此 G/G'

为 $(2^{n-1},2,2)$ 型交换群. 注意到 $\Omega_1(G)\leqslant Z$，则存在 $w\in G\backslash A$ 且 $o(w)=4$. 令 $u^w=uz_1$, $v^w=vz_2$, $w^2=z_3$, 其中 $z_1,z_2,z_3\in G'$.

易证映射 $a\longmapsto a^{w+1}$ 为 A 到 A^{w+1} 上的同态映射且 $(u^2)^{w+1}=u^4\neq 1$. 若 $z_3\in A^{w+1}$, 则存在 $a\in A$ 使得 $a^{w+1}=z_3$. 从而 $(wa)^2=wawa=w^2a^{w+1}=z_3^2=1$, 矛盾. 故 A^{w+1} 循环. 又因为 $n\geqslant 3$, 所以 $u^{2^{n-1}}$ 为其唯一的 2 阶元. 注意到映射 $a\to a^{w+1}$ 的核包含 G' 但不包含 $\langle u^{2^{n-2}}\rangle$. 由于 A^{w+1} 循环, 不妨设 $v^{w+1}=1$, 即 $v^w=v^{-1}$. 又因为 $z_3\notin A^{w+1}$, 所以可设 $z_3=v^2$ 或者 $z_3=v^2u^{2^{n-1}}$. 不失一般性, 总可用 $wu^{2^{n-2}}$ 替换 w 可得, $w^2=v^2$. 从而 $B=\langle v,w\rangle\cong \mathrm{Q}_8$. 又因为 B 非循环, 所以 $B\lhd G$. 因此 $z_1\in\Omega_1(B)=\langle v^2\rangle$. 故 $G'\leqslant\langle v^2\rangle$, 矛盾.

最后, 我们来验证型 (i)—(iii) 均满足 $\mathrm{chn}(G)\leqslant 1$, 而 (iv), (v) 中也存在一些满足 $\mathrm{chn}(G)\leqslant 1$ 的群, 但不属于群 (i)—(iii) 之一. 设 G 为群 (i) 或 (iii), 则 $|G'|=p$. 故由 [181] 中的引理 1.5 知 $G/Z(G)$ 初等交换. 若 G 为群 (i), 则令 B 为 G 的循环正规子群且使得 G/B 循环. 若 G 为群 (iii), 则令 $B=\mathrm{Q}_8\leqslant G$. 设 $H\ntrianglelefteq G$, 则 $G'\nleqslant H$. 又因为 $|G'|=p$, 所以 $H\bigcap G'=1$. 由于 B 选取的任意性, 因此总可设 $H\bigcap B=1$. 进而 $H\cong G/B$. 故 H 循环. 由于 $G/Z(G)$ 初等交换, 因此 H 的每个子群均在 G 中正规. 故 $\mathrm{chn}(G)\leqslant 1$. 设 G 为群 (ii), 则 G 的所有阶 $\geqslant p^2$ 的子群均正规, 从而 $\mathrm{chn}(G)=1$. 下面我们来考虑一些特殊的情形. 当 $p=2$ 时, 考虑群 $G\cong\mathrm{Q}_{16}$. 此时, $\mathrm{chn}(G)=1$, 但 $|G'|=4$. 显然 G 不属于群 (i)—(iii) 之一. 当 $p=3$ 时, 令 G 为 [89] 中的例子 III.10.15 中的群, 容易证明 $\mathrm{chn}(G)=1$ 且 $c(G)=3$. 显然 G 不属于群 (i)—(iii) 之一. □

对于定理 11.1.4 中 (iv) 型群, 宋蕾薇和曲海鹏[205] 以及 Berkovich 和 Janko 在 [26] 中的 §16 分别独立地给出了其分类. 结果如下.

定理 11.1.5 设 G 为阶 $\leqslant 2^7$ 的有限 2 群. 若 G 的所有非正规子群均循环且 G 不属于定理 11.1.4 中的 (i)—(iii) 型群之一, 则 G 同构于以下群之一.

(1) $\mathrm{D}_8*\mathrm{Q}_8$;

(2) Q_{16};

(3) $\langle a,b\mid a^8=1,b^4=a^4,[a,b]=a^{-2}\rangle$;

(4) $\langle a,b,c\mid a^4=1,b^2=a^2,c^4=1,[a,b]=a^2c^2,[a,c]=1,[b,c]=c^2\rangle$;

(5) $\langle a,b,c,d\mid a^4=b^4=1,c^2=a^2b^2,d^2=a^2,[a,b]=a^2,[c,d]=a^2b^2,[b,c]=[a,d]=b^2,[a,c]=[b,d]=1\rangle$.

对于定理 11.1.4 中的 (v) 型群, 不难得到如下定理.

定理 11.1.6 设 G 为 3^4 阶非正则群. 若 G 的所有非正规子群皆循环, 则 $G=\langle a,b,c\mid a^9=c^3=1,b^3=a^3,[a,b]=c,[c,a]=1,[c,b]=a^{-3}\rangle$.

对于定理 11.1.4—定理 11.1.6 的结论, 我们有下列定理.

定理 11.1.7　设 G 是非 Dedekind p 群. 则 G 的所有非正规子群均为 p 阶当且仅当 G 为下列互不同构的群之一.

(1) $\mathrm{M}_p(m,1)$;

(2) $\mathrm{D}_8 * \mathrm{C}_{2^n}, n \geqslant 2$;

(3) $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n}, p > 2$;

(4) $\mathrm{Q}_8 * \mathrm{D}_8$.

张丽华等在文献 [263] 减弱 Passman 的条件 "非正规子群均循环" 为 "非正规交换子群均循环", 并分类了具有这种性质的 p 群. 分类结果如下.

定理 11.1.8　设 G 是有限非 Dedekind p 群, $p > 2$. 则 G 的非正规交换子群均循环当且仅当 G 是下列群之一.

(i) $\mathrm{M}_p(m,n)$;

(ii) $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n}$;

(iii) $\langle a, b \mid a^9 = c^3 = 1, b^3 = a^3, [a,b] = c, [c,a] = a^3, [c,b] = 1\rangle$.

定理 11.1.9　设 G 是有限非 Dedekind 2 群, $|G| \geqslant 2^7$. 则 G 的非正规交换子群均循环当且仅当 G 是下列群之一.

(1) $\mathrm{M}_2(m,n)$, $n+m \geqslant 7$;

(2) Q_{2^n}, $n \geqslant 7$;

(3) $\langle a, b \mid a^{2^{n+1}} = 1, b^4 = a^{2^n}, [a,b] = a^{-2}\rangle$, $n \geqslant 4$;

(4) $\mathrm{Q}_8 \times \mathrm{C}_{2^n}$, $n \geqslant 4$;

(5) $\mathrm{D}_8 * \mathrm{C}_{2^n}$, $n \geqslant 5$;

(6) $\langle a, b, c \mid a^4 = 1, b^{2^n} = 1, a^2 = c^2, [a,b] = 1, [a,c] = a^2, [b,c] = b^{2^{n-1}}\rangle$, $n \geqslant 4$.

11.2　非正规子群均同阶的 p 群

Zappa[253, 254] 确定了非正规子群均同阶的有限群. 对于 p 群, 不难证明, 群 G 的所有非正规子群同阶可推出 G 的所有非正规子群循环. Berkovich 在文献 [28] 中的定理 112.3、定理 112.4 给出了非正规子群均同阶的 p 群分类. 当 $p=2$ 时, 张军强 [259] 独立地给出了非正规子群均同阶的 2 群分类的一个新证明, 也给出了非正规子群均同阶的有限群的结构. 王丽芳[230] 分类了非正规内交换子群均同阶的亚循环 2 群. 本节的证明取自 [259].

定理 11.2.1　设 G 是有限 2 群. 则 G 的所有非正规子群的阶都为 2^2 当且仅当 G 同构于下列互不同构的群之一.

(1) $\mathrm{M}_2(m,2) = \langle a, b \mid a^{2^m} = b^4 = 1, [a,b] = a^{2^{m-1}}\rangle$;

(2) $\mathrm{Q}_8 \times \mathrm{C}_4$;

(3) Q_{16};

(4) $\langle a, b, c \mid a^4 = b^4 = 1, c^2 = b^2, [a, b] = 1, [a, c] = b^2, [b, c] = a^2 \rangle$;

(5) $\langle a, b, c, d \mid a^4 = b^4 = 1, a^2 = d^2 = [a, b], c^2 = [c, d] = a^2b^2, [b, c] = [a, d] = b^2, [a, c] = [b, d] = 1 \rangle$.

证明 $\Longrightarrow$: 由假设可知, G 的所有 2 阶子群都正规. 从而 $\Omega_1(G) \leqslant Z(G)$. 若 $|G'| \geqslant 2^3$, 由引理 11.1.2 可知, 存在 G' 的极大子群 K 使得 $K \trianglelefteq G$ 且 G/K 不是 Dedekind 群. 于是存在 $H/K \ntrianglelefteq G/K$. 由对应定理可得 $H \ntrianglelefteq G$ 且 $|H| > |K| \geqslant 2^2$, 矛盾. 故 $|G'| \leqslant 2^2$. 因为 G 存在非正规子群, 故 $G' \neq 1$. 于是 $|G'| = 2$ 或者 $|G'| = 2^2$. 分两种情况讨论.

情形 1 $|G'| = 2$.

设 H 是 G 的内交换子群. 由定理 1.7.10 可知, H 同构于 Q_8, $\mathrm{M}_2(m, n)$ 或者 $\mathrm{M}_2(m, n, 1)$. 因为 H 的非正规子群, 如果存在的话, 也都为 4 阶. 不难得到 H 同构于 Q_8 或者 $\mathrm{M}_2(m, 2)$.

若 $H \cong \mathrm{Q}_8$, 由引理 10.1.1 可知 $G = H * C_G(H)$. 不妨设

$$H = \langle a, b \mid a^4 = 1, b^2 = a^2, [a, b] = a^2 \rangle.$$

若存在 $x \in C_G(H) \setminus H$ 使得 $o(x) = 2^2$ 且 $x^2 = a^2 = b^2$, 则 $(xa)^2 = 1$ 且 $xa \notin Z(G)$, 这矛盾于 $\Omega_1(G) \leqslant Z(G)$. 故对 $C_G(H) \setminus H$ 中的任意的 2^2 阶元 x 均有 $\langle x \rangle \bigcap H = 1$. 若存在 $x \in C_G(H) \setminus H$ 使得 $o(x) = 2^3$, 则 $\langle x \rangle \bigcap H = 1$. 从而 $\langle xa \rangle$ 或者 $\langle xb \rangle$ 是一个 2^3 阶的非正规子群, 矛盾. 于是对任意的 $x \in C_G(H) \setminus H$ 都有 $o(x) \leqslant 2^2$. 我们断言 $G = H \times \langle x \rangle$, 其中 x 是 $C_G(H) \setminus H$ 中的一个 2^2 阶元. 若否, 存在 $C_G(H) \setminus H$ 中的 2 阶元 y 使得 $\langle y \rangle \bigcap (H \times \langle x \rangle) = 1$. 则 $\langle xa, y \rangle$ 是一个 2^3 阶非正规子群, 矛盾. 故 $G \cong \mathrm{Q}_8 \times \mathrm{C}_4$, 即得定理中的群 (2).

假设 G 不存在内交换子群同构于 Q_8, 则 H 同构于 $\mathrm{M}_2(m, 2)$. 由引理 10.1.1 可知 $G = H * C_G(H)$. 不妨设

$$H = \langle a, b \mid a^{2^m} = b^4 = 1, [a, b] = a^{2^{m-1}} \rangle, \quad m \geqslant 2.$$

我们断言 $C_G(H) \leqslant H$. 若否, 选择 $x \in C_G(H) \setminus H$ 使得 $\overline{M} = \langle \overline{a} \rangle \times \langle \overline{b} \rangle \times \langle \overline{x} \rangle$, 其中 $M = \langle H, x \rangle$ 且 $\overline{M} = M/G'$, $\overline{a}^{2^{m-1}} = \overline{b}^4 = \overline{x}^{2^{n-1}} = \overline{1}$, $n \geqslant 2$. 那么 $x^{2^{n-1}} = 1$ 或者 $x^{2^{n-1}} = a^{2^{m-1}}$. 若 $x^{2^{n-1}} = 1$, 则 $|\langle b, x \rangle| \neq 2^2$ 且 $\langle b, x \rangle \ntrianglelefteq G$, 矛盾. 于是 $x^{2^{n-1}} = a^{2^{m-1}}$. 若 $m = 2$, 则 $ax^{2^{n-2}} \notin Z(G)$ 且 $(ax^{2^{n-2}})^2 = a^2x^{2^{n-1}} = a^4 = 1$, 这矛盾于 $\Omega_1(G) \leqslant Z(G)$. 于是 $m > 2$. 我们得到 $(a^{2^{m-2}}x^{2^{n-2}})^2 = 1$. 从而 $\langle b, a^{2^{m-2}}x^{2^{n-2}} \rangle \ntrianglelefteq G$ 且 $|\langle b, a^{2^{m-2}}x^{2^{n-2}} \rangle| = 2^3$, 矛盾. 所以 $C_G(H) \leqslant H$. 从而 $G \cong \mathrm{M}_2(m, 2)$. 这即为定理中的群 (1).

情形 2 $|G'| = 2^2$.

由引理 11.1.2, 存在 G' 的极大子群 K 使得 G/K 非 Dedekind 群. 对任意的 $H/K \ntrianglelefteq G/K$ 有 $H \ntrianglelefteq G$. 则 $|H| = 2^2$ 且 $|H/K| = 2$, 从而 $\overline{G} = G/K$ 的非正规子群

的阶都为 2. 由定理 11.1.7 可得 G/K 同构于 $\mathrm{M}_2(m,1)$, $\mathrm{D}_8 * \mathrm{C}_{2^n}$, 或者 $\mathrm{D}_8 * \mathrm{Q}_8$. 以下分这三种情况讨论.

子情形 2.1　$G/K \cong \mathrm{M}_2(m,1)$.

不妨设 $G/K = \langle \overline{a}, \overline{b} \mid \overline{a}^{2^m} = 1, \overline{b}^2 = 1, [\overline{a}, \overline{b}] = \overline{a}^{2^{m-1}} \rangle$. 因为 $K \leqslant G'$, 由 [24] 中的定理 2 可得 G 亚循环. 从而 $G' \leqslant \langle a \rangle$ 且 $\langle a \rangle$ 是 G 的一个循环极大子群. 由定理 1.9.1 可得 $G \cong \mathrm{Q}_{16}$. 这即为定理中的群 (3).

子情形 2.2　$G/K \cong \mathrm{D}_8 * \mathrm{C}_{2^n}$.

不妨设 $G/K = \langle \overline{a}, \overline{b}, \overline{c} \mid \overline{a}^{2^n} = 1, \overline{b}^2 = \overline{c}^2 = 1, [\overline{b}, \overline{c}] = \overline{a}^{2^{n-1}}, [\overline{a}, \overline{b}] = [\overline{a}, \overline{c}] = 1 \rangle$, 其中 $n \geqslant 2$. 令 $K = \langle e \rangle$. 则 $e \in Z(G)$ 且

$$G = \langle a, b, c \mid a^{2^n} = e^i, b^2 = e^j, c^2 = e^k, [b, c] = a^{2^{n-1}} e^u, [a, b] = e^s, [a, c] = e^t \rangle,$$

其中 $i, j, k, u, s, t = 0$ 或者 1, $n \geqslant 2$. 因为 $b, c \notin Z(G)$, 所以由 $\Omega_1(G) \leqslant Z(G)$ 可得 $b^2 = c^2 = e$. 若 $a^{2^n} = e$, 则存在 $b_1 = ba^{2^{n-1}}$ 使得 ${b_1}^2 = 1$ 且 $b_1 \notin Z(G)$, 矛盾. 因此 $o(a) = 2^n$ 且 $G' = \langle a^{2^{n-1}} \rangle \times \langle b^2 \rangle$. 从而 $[a, b] \neq 1$ 或者 $[a, c] \neq 1$. 所以 $\langle a \rangle \ntrianglelefteq G$. 这意味着 $n = 2$. 于是

$$G = \langle a, b, c \mid a^4 = b^4 = 1, c^2 = b^2, [b, c] = a^2 b^{2u}, [a, b] = b^{2s}, [a, c] = b^{2t} \rangle,$$

其中 $u, s, t = 0$ 或者 1, 且 $G' = Z(G) = \Omega_1(G) = \langle a^2 \rangle \times \langle b^2 \rangle$.

若 $[a, b] = 1$, 则由 $G' = \langle a^2 \rangle \times \langle b^2 \rangle$ 可得 $[a, c] = b^2$. 因为 $abc \notin Z(G)$, 所以 $(abc)^2 = a^2 b^2 c^2 [a, b][a, c][b, c] = b^2 b^{2u} \neq 1$. 于是 $u = 0$. 从而

$$G = \langle a, b, c \mid a^4 = b^4 = 1, c^2 = b^2, [b, c] = a^2, [a, b] = 1, [a, c] = b^2 \rangle.$$

这即为定理中的群 (4).

若 $[a, b] = b^2, [a, c] = 1$, 与上面情形同理可得 $[b, c] = a^2$. 令 $c_1 = b, b_1 = c$, 则 $G = \langle a, b_1, c_1 \rangle$ 且同构于定理中的群 (4). 若 $[a, b] = b^2, [a, c] = b^2$, 类似可得 $[b, c] = a^2 b^2$. 令 $b_1 = abc$. 则 $G = \langle a, b_1, c \rangle$ 且同构于定理中的群 (4).

子情形 2.3　$G/K \cong \mathrm{D}_8 * \mathrm{Q}_8$.

不妨设

$$G/K = \langle \overline{a}, \overline{b}, \overline{c}, \overline{d} \mid \overline{a}^4 = \overline{b}^2 = \overline{1}, [\overline{a}, \overline{b}] = \overline{a}^2, \overline{c}^2 = \overline{d}^2 = \overline{a}^2, \\ [\overline{c}, \overline{d}] = \overline{d}^2, [\overline{a}, \overline{c}] = [\overline{a}, \overline{d}] = [\overline{b}, \overline{c}] = [\overline{b}, \overline{d}] = \overline{1} \rangle.$$

令 $K = \langle e \rangle$. 则 $e^2 = 1, e \in Z(G)$ 且

$$G = \langle a, b, c, d \mid a^4 = e^i, b^2 = e^j, c^2 = a^2 e^k, d^2 = a^2 e^l, [a, b] = a^2 e^u, [a, c] = e^s, \\ [a, d] = e^t, [b, c] = e^r, [b, d] = e^x, [c, d] = d^2 e^y \rangle,$$

其中 $i, j, k, l, u, s, t, r, x, y = 0$ 或者 1.

首先, 可设 $[a,c]=1$, 即 $s=0$. 其次可证 $j=1, i=0, u=0$ 且 $k=1$. 因为 $[a,b]\neq 1$ 且 $b\notin Z(G)$, 所以由 $\Omega_1(G)\leqslant Z(G)$ 可得 $b^2=e$, 即 $j=1$. 若 $a^4=e$, 则 $o(a)=o(c)=o(d)=8$. 由于 $|\langle c,d\rangle|=16$, 故 $\langle c\rangle\trianglelefteq\langle c,d\rangle$ 且 $\langle d\rangle\trianglelefteq\langle c,d\rangle$. 所以 $\langle c,d\rangle$ 为 16 阶的 Dedekind 2 群, 矛盾. 所以 $a^4=1$, 即 $i=0$. 由于 $[a^2,b]=[a^2,c]=[a^2,d]=1$, 故 $Z(G)=G'=\langle a^2\rangle\times\langle b^2\rangle$. 因为 $ab\notin Z(G)$, 所以 $(ab)^2=a^2b^2[b,a]\neq 1$. 从而 $[a,b]=a^2$, 即 $u=0$. 类似地, 由 $ac\notin Z(G)$ 可得 $c^2=a^2b^2$, 即 $k=1$.

再者可证 $y=1, l=0, t=1$ 且 $r=1$. 由 $\Omega_1(G)\leqslant Z(G)=G'=\langle a^2\rangle\times\langle b^2\rangle$ 得

$$(dac)^2=d^2a^2c^2[d,a][d,c]=a^2b^{2l}\cdot a^2\cdot a^2b^2\cdot b^{2t}\cdot a^2b^{2y}=b^{2(1+l+t+y)}\neq 1.$$

于是 $l+t+y=0$ 或者 2. 类似地,

$$(da)^2=d^2a^2[d,a]=a^2b^{2l}\cdot a^2\cdot b^{2t}=b^{2(l+t)}\neq 1.$$

所以 $l+t=1$. 从而 $y=1, [c,d]=a^2b^2$. 若 $l=1$, 则 $\mathrm{Q}_8\cong\langle c,d\rangle\trianglelefteq G$. 从而 $\langle c,d\rangle^b=\langle c,d\rangle$. 于是 $[b,c]=[b,d]=1$. 由此可得 $\langle a,bc\rangle\cong\mathrm{Q}_8$. 因此 $\langle a,bc\rangle\trianglelefteq G$. 而 $(bc)^d=bc^d=a^2b^{-1}c\notin\langle a,bc\rangle$, 矛盾. 所以 $l=0$. 从而 $t=1$, 即 $d^2=a^2$, $[a,d]=b^2$. 若 $r=0$ 且 $[b,c]=1$, 则 $\mathrm{Q}_8\cong\langle a,bc\rangle\ntrianglelefteq G$. 而 $[d,a]=b^2\notin\langle a,bc\rangle$, 矛盾. 所以 $r=1$ 且 $[b,c]=b^2$.

最后, 可设 $[b,d]=1$, 即 $x=0$. 事实上, 若 $x=1, [b,d]=b^2$, 令 $d_1=cd$, 则 $[b,d_1]=[b,cd]=[b,c][b,d]=1$, 而其他定义关系也都不变.

综上可得, $G\cong\langle a,b,c,d\mid a^4=b^4=1, a^2=d^2=[a,b], c^2=[c,d]=a^2b^2, [b,c]=[a,d]=b^2, [a,c]=[b,d]=1\rangle$. 这即为定理中的群 (5).

$\Longleftarrow$: 显然, 群 (1)—(5) 互不同构. 我们证明群 (1)—(5) 的非正规子群同阶.

设 G 为群 (1), H 是 G 的非正规子群. 则 $G'\nleqslant H$. 从而 $\langle a\rangle\bigcap H=1$. 于是

$$H\cong H/(\langle a\rangle\bigcap H)\cong\langle a\rangle H/\langle a\rangle\leqslant G/\langle a\rangle,$$

且 $|H|\leqslant|G/\langle a\rangle|=2^2$. 由 $\Omega_1(G)\leqslant Z(G)$ 可得 $|H|=2^2$.

若 G 为群 (2), 设 $G=\langle a,b,c\mid a^4=c^4=1, b^2=a^2, [a,b]=a^2, [a,c]=[b,c]=1\rangle$. 易得 $|G|=2^5$ 且 $\Omega_1(G)\leqslant Z(G)$. 于是只需考虑 G 的 2^3 阶子群 H. 因为 $H\bigcap\langle a,b\rangle\neq 1$ 且 $\langle a,b\rangle$ 的 2 阶子群为 G', 所以 $G'\leqslant H$. 于是 $H\trianglelefteq G$. 另一方面, G 有 4 阶非正规子群 $\langle ac\rangle$. 所以群 (2) 满足假设.

若 G 为群 (3), 设 $G=\langle a,b\mid a^8=1, b^2=a^4, a^b=a^{-1}\rangle$. 因为 $\Omega_1(G)=Z(G)=\langle a^4\rangle$ 且 $\langle b\rangle$ 是 G 的一个 4 阶非正规子群, 所以群 (3) 满足假设.

若 G 为群 (4), 则 $G\cong\langle a,b,c\mid a^4=b^4=1, c^2=b^2, [a,b]=1, [a,c]=b^2, [b,c]=a^2\rangle$. 易见 $\Omega_1(G)=Z(G)=G'=\langle a^2\rangle\times\langle b^2\rangle$. 对 G 的任意非正规子群 H, 存在 $K\leqslant G'\bigcap H$ 使得 $K=\langle a^2\rangle, \langle b^2\rangle$ 或者 $\langle a^2b^2\rangle$, 所以

$G/\langle a^2\rangle=\langle \bar{a},\bar{b},\bar{c}\mid \bar{a}^2=\bar{b}^4=1,\bar{b}^2=\bar{c}^2,[\bar{a},\bar{b}]=1,[\bar{a},\bar{c}]=\bar{b}^2,[\bar{b},\bar{c}]=1\rangle\cong \mathrm{D}_8*\mathrm{C}_4;$

$G/\langle b^2\rangle=\langle \bar{a},\bar{b},\bar{c}\mid \bar{a}^4=\bar{b}^2=\bar{c}^2=1,[\bar{a},\bar{b}]=[\bar{a},\bar{c}]=1,[\bar{b},\bar{c}]=\bar{a}^2\rangle\cong \mathrm{D}_8*\mathrm{C}_4.$

令 $a'=ab$. 则

$$G=\langle a',b,c\mid a'^4=b^4=1,b^2=c^2,[a'b]=1,[a',c]=a'^2,[b,c]=a'^2b^2\rangle.$$

从而

$$G/\langle a^2b^2\rangle=\langle \overline{a'},\bar{b},\bar{c}\mid \overline{a'}^2=\bar{b}^4=1,\bar{b}^2=\bar{c}^2,[\overline{a'},\bar{b}]=[\overline{a'},\bar{c}]=1,[\bar{b},\bar{c}]=\bar{b}^2\rangle.$$

显然, $G\cong \mathrm{Q}_8\times\mathrm{C}_2$. 于是 G 是 Dedekind 2 群. 由定理 11.1.7 可得 $G/\langle a^2\rangle$ 和 $G/\langle b^2\rangle$ 的非正规子群都为 2 阶. 所以 H/K 是一个 2 阶非正规子群, 从而 H 是一个 4 阶非正规子群. 群 (4) 满足假设.

若 G 为群 (5), 类似地可得 G 的非正规子群都为 4 阶. 群 (5) 满足假设. □

定理 11.2.2 设 G 是有限 2 群. 则 G 的所有非正规子群为 $2^m(m\geqslant 3)$ 阶当且仅当 $G\cong \mathrm{M}_2(n,m)$, 其中 $n\geqslant m\geqslant 3$.

证明 假设 G 的所有非正规子群都为 2^m 阶, 其中 $m\geqslant 3$. 对任意的 $H\ntrianglelefteq G$ 可得 H 循环. 由 [181] 中的命题 1.3 可得 $Z(G)/H\bigcap Z(G)$ 循环. 从而 $Z(G)$ 亚循环. 由 [181] 中的命题 1.6 可得 $\Omega_2(G)\leqslant Z(G)$. 所以 $\Omega_2(G)$ 亚循环. 由定理 8.1.1 可得 G 亚循环.

因为 G 的所有非正规子群都循环, 所以由 $\Omega_1(G)\cong \mathrm{C}_2^2$ 可得 $G/\Omega_1(G)$ 为 Dedekind 2 群. 若 $G/\Omega_1(G)$ 非交换, 则由 G 亚循环可得 $G/\Omega_1(G)\cong \mathrm{Q}_8$. 令 $G/\Omega_1(G)=\langle \bar{a},\bar{b}|\bar{a}^4=1,\bar{a}^2=\bar{b}^2=[\bar{a},\bar{b}]\rangle$. 则 $a^2=b^2z, z\in\Omega_1(G)$, $a^2\in Z(G)$. 这意味着 $|Z(G)|\geqslant|\langle a^2,\Omega_1(G)\rangle|=2^3$. 因为 G 非交换, 所以 $|Z(G)|=2^3$. 因此 G 有交换极大子群. 由定理 1.7.6 可得 $|G'|=2$, 这矛盾于 $G/\Omega_1(G)$ 非交换. 因此 $G/\Omega_1(G)$ 交换且 $|G'|=2$, 即 G 是一个亚循环内交换 2 群. 因为 $\mathrm{M}_2(n,2)$ 和 $\mathrm{M}_2(n,1)$ 有阶 $<2^3$ 的非正规子群, 不妨设

$$G=\langle a,b\mid a^{2^n}=1,b^{2^m}=1,[a,b]=a^{2^{n-1}}\rangle,$$

其中 $m\geqslant 3$. 若 $n<m$, 则存在非正规子群 $H_1=\langle ab^{2^{m-n}}\rangle$ 和 $H_2=\langle b\rangle$. 而 $|H_1|=2^n\neq|H_2|$, 矛盾. 于是 $n\geqslant m$. 下面我们证明 G 的非正规子群都为 2^m 阶. 事实上, 设 H 为 G 的任一非正规子群, 则 $G'\nleqslant H$. 从而 $\langle a\rangle\bigcap H=1$. 由于 $\langle a\rangle H/\langle a\rangle\leqslant G/\langle a\rangle$ 且 $\langle a\rangle H/\langle a\rangle\cong H/\langle a\rangle\bigcap H$, 所以 $|H|\leqslant|G/\langle a\rangle|=2^m$. 若 $|H|<2^m$, 则 $H\leqslant\Omega_{m-1}(G)\leqslant Z(G)$, 矛盾. 所以 $|H|=2^m$. 结论成立. □

定理 11.2.3 设 G 是有限非 Dedekind 群. 若 G 的所有非正规子群的阶相同, 则 G 是 p 群或 $G\cong \mathrm{C}_q\rtimes\mathrm{C}_{p^m}$, 其中 $m\geqslant 1$, $q\neq 2$. 若 $G\cong \mathrm{C}_q\rtimes\mathrm{C}_{p^m}$, 则 G 的所有非正规子群的阶为 p^m.

证明 设 P_i 是 G 的 Sylow p_i 子群, 其中 $|P_i| = {p_i}^{n_i}$, $i = 1, 2, \cdots, s$.

若 G 的非正规子群的阶不等于任何一个 Sylow 子群的阶, 则 G 的 Sylow 子群均正规, 从而 G 幂零. 设 $G = P_1 \times P_2 \times \cdots \times P_s$. 下证 G 为 p 群.

设 K 为 G 的一个非正规子群. 首先断言: $|K| = p^n$, 其中对每个 i 均有 $n < n_i$. 若否, 不妨设 $|K| = {p_1}^{s_1}{p_2}^{s_2}$. 于是存在 K_1 , $K_2 \leqslant G$ 使得 $K_1 \times K_2 \ntrianglelefteq G$, 其中 $|K_j| = {p_j}^{s_j}$, $1 \leqslant s_j \leqslant n_j$, $j = 1, 2$. 由假设得 $K_j \trianglelefteq G$, 从而 $K_1 \times K_2 \trianglelefteq G$, 矛盾. 其次我们断言 $s \leqslant 2$. 若否, 不妨设 $G = P_1 \times P_2 \times P_3$. 令 $H \ntrianglelefteq G$ 且 $H < P_1$. 于是 $\langle H, P_2\rangle \trianglelefteq G$ 且 $\langle H, P_3\rangle \trianglelefteq G$. 由此可得 $\langle H, P_2\rangle \bigcap \langle H, P_3\rangle = H \trianglelefteq G$, 矛盾. 最后我们证明 $s = 1$. 若否, 设 $G = P_1 \times P_2$. 若 $H \times P_2 \trianglelefteq G$, 则对于 $g \in G$, $H^g P_2 = HP_2$. 于是由 $H^g P_2/P_2 = HP_2/P_2$ 且 $H^g/H^g \bigcap P_2 = H/H \bigcap P_2$ 可得 $H^g = H$, 即 $H \trianglelefteq G$, 这矛盾于 $H \ntrianglelefteq G$. 于是 $H \times P_2 \ntrianglelefteq G$, 矛盾, 即证得 G 是 p 群.

若 G 的非正规子群的阶等于某个 Sylow 子群 P 的阶, 不妨设 $P = P_s$. 则当 $|P_i| \neq |P|$ 时就有 $P_i \trianglelefteq G$. 于是 $G = (P_1 \times P_2 \times \cdots \times P_{s-1}) \rtimes P$. 若 $s \geqslant 3$, 则 $P_1 \rtimes P \trianglelefteq G$ 且 $P_2 \rtimes P \trianglelefteq G$. 于是 $P = (P_1 \rtimes P) \bigcap (P_2 \rtimes P) \trianglelefteq G$, 矛盾. 故 $s = 2$. 为方便令 $P_1 = Q$, 其中 $|Q| = q^j$, $q \neq p$. 则 $G = Q \rtimes P$. 因为 $P \ntrianglelefteq G$ 且 G 的所有非正规子群同阶, 由此得 P 循环. 若 Q 有两个不同的 q 阶子群 M_1 和 M_2, 则 $\langle M_1, P\rangle \trianglelefteq G$ 且 $\langle M_2, P\rangle \trianglelefteq G$. 于是 $P = \langle M_1, P\rangle \bigcap \langle M_2, P\rangle \trianglelefteq G$, 矛盾. 故 Q 有唯一的 q 阶子群. 从而 Q 循环或为广义四元数群. 由假设可知 Q 的所有真子群是 G 的正规子群, 故 Q 是 Dedekind 2 群, 即 $Q \cong \mathrm{Q}_8$. 于是存在 $K \leqslant Q$ 使得 $|K| = 2$, 有 $KP \trianglelefteq G$. 由此可知, 对 $g \in G$, $KP^g/K = KP/K$ 且 $P^g/K \bigcap P^g = P/K \bigcap P$. 这推出 $P^g = P$, 矛盾. 故 Q 循环.

令 $Q = \langle a\rangle$ 且 $P = \langle b\rangle$, 其中 $o(a) = q^n$, $o(b) = p^m$. 下证 $n \neq 1$. 若否, 令 $\overline{G} = G/\langle a^{q^{n-1}}\rangle$. 因为 $\langle a^{p^{n-1}}\rangle P \trianglelefteq G$, 故 $\overline{P} \trianglelefteq \overline{G}$. 从而 $\overline{G}$ 交换. 于是 $G' \leqslant \langle a^{q^{n-1}}\rangle$. 因为 $[a^{q^{n-1}}, b] = [a, b]^{q^{n-1}} = 1$, 故 $\langle a^{q^{n-1}}\rangle \leqslant Z(G)$. 由此可得 G 幂零, 矛盾. 于是 $n = 1$. 若 $q = 2$, 则 $|G : P| = 2$. 由此可得 $P \trianglelefteq G$, 矛盾. 故 $q \neq 2$.

反之, 设 $H \leqslant G$ 且 $|H| \neq p^m$. 若 $q \mid |H|$, 则 $\langle a\rangle = G' \leqslant H$. 从而 $H \trianglelefteq G$. 若 $q \nmid |H|$, 则 $|H| \leqslant p^{m-1}$. 从而 $H \leqslant \langle b^p\rangle = Z(G)$. 也有 $H \trianglelefteq G$. 由此证得 G 的非正规子群的阶是 p^m. □

11.3 非正规子群的阶至多为 p^2 的 p 群

沿着 Passman 的路线, 张勤海等[275] 确定了非正规子群的阶为 p 或 pq 的有限群的结构, 其中 p, q 是素数; 作为推论, 也确定了非正规子群均循环的有限群的结构; 对于 p 群, 分类了非正规子群的阶不超过 p^2 的 p 群. 本节的内容取自 [275].

为叙述简便, 以下我们假设所讨论的 p 群 G 满足: G 的阶 $\geqslant p^3$ 的子群均正规且 G 至少有一个 p^2 阶非正规子群. 记这样的群为 $\mathcal{N}_2$ 群.

下面我们对满足上述假设的 p 群进行分类.

命题 11.3.1 $\mathrm{Q}_8 * \mathrm{C}_{2^m} \cong \mathrm{D}_8 * \mathrm{C}_{2^m} \leqslant \mathrm{Q}_8 * \mathrm{M}_p(m,n)$, 其中 $\mathrm{Q}_8 \bigcap \mathrm{M}_p(m,n) = \mathrm{M}_p'(m,n)$, $m \geqslant 2$.

证明 由 $\mathrm{Q}_8 * \mathrm{C}_4 \cong \mathrm{D}_8 * \mathrm{C}_4$ 即得. □

命题 11.3.2 设 $G = M * C$, 其中 $M \cong \mathrm{M}_p(m,1)$, $C \cong \mathrm{C}_{p^n}$. 再设 $M \bigcap C \cong \mathrm{C}_{p^i}$, $1 \leqslant i \leqslant n-1$. 则

(1) 若 $m > n$, 则 $G \cong \mathrm{M}_p(m,1) \times \mathrm{C}_{p^{n-i}}$;

(2) 若 $m \leqslant n$, 则 $G \cong \mathrm{M}_p(m-i,1,1) * \mathrm{C}_{p^n}$, 其中 $\mathrm{M}_p(m-i,1,1) \bigcap \mathrm{C}_{p^n} = \mathrm{M}_p(m-i,1,1)'$.

证明 设 $M = \langle a, b \mid a^{p^m} = b^p = 1, a^b = a^{1+p^{m-1}} \rangle$. 则 $Z(M) = \langle a^p \rangle$. 因为 $M \bigcap C \cong \mathrm{C}_{p^i}$, 令 $C = \langle c \rangle$, 不妨设 $c^{p^{n-i}} = a^{p^{m-i}}$. 若 $m > n$, 令 $c_1 = ca^{-p^{m-n}}$. 则 $o(c_1) = p^{n-i}$ 且 $G = M \times \langle c_1 \rangle$. 此时 (1) 成立. 若 $m \leqslant n$, 令 $a_1 = ac^{-p^{n-m}}$. 则 $o(a_1) = p^{m-i}$ 且 $M_1 = \langle a_1, b \rangle \cong \mathrm{M}_p(m-i,1,1)$. 我们有 $G = M_1 * C$ 且 $M_1 \bigcap C = \langle a^{p^{m-1}} \rangle = M_1'$, 此时 (2) 成立. □

引理 11.3.3 设 G 是 $\mathcal{N}_2$ 群. 则 $|G'| \leqslant p^2$.

证明 设 $|G'| > p^2$. 由引理 11.1.2 可知, G 有一个满足 $|G' : K| = p$ 的正规子群 K 使得 G/K 不是 Dedekind 群. 于是 G/K 有一个非正规子群 H/K. 由此可得 $H \ntrianglelefteq G$. 因为 $|K| \geqslant p^2$, 故 $|H| \geqslant p^3$. 矛盾. □

引理 11.3.4 设 $|G'| = p$, $H \leqslant G$, H 不是 Dedekind 群且 $Z(H)$ 循环. 则 $C_G(H)$ 的阶 $\geqslant p^2$ 的子群均是 G 的正规子群.

证明 显然, $G' = H'$ 是 $Z(H)$ 的唯一的 p 阶子群. 设 $N \leqslant C_G(H)$, $|N| = p^2$ 且 $N \ntrianglelefteq G$. 令 $M \ntrianglelefteq H$. 则 $M \nleqslant C_G(H)$. 于是 $M \nleqslant N$. 由此可得 $|MN| \geqslant p^3$ 且 $MN \trianglelefteq G$. 因为 $MN \nleqslant Z(G)$, 由命题 5.4.2 可得 $G' \leqslant MN$. 于是 $G' \leqslant MN \bigcap H = M(N \bigcap H)$. 又因为 $N \ntrianglelefteq G$, 故 $G' \nleqslant N \bigcap H \leqslant Z(H)$. 由此可得 $N \bigcap H = 1$. 因而 $G' \leqslant M$ 且 $M \trianglelefteq G$, 矛盾. □

定理 11.3.5 G 是具有 $|G'| = p$ 的 $\mathcal{N}_2$ 群当且仅当 G 同构于下列互不同构的群之一.

(i) $\mathrm{M}_p(1,1,1) * \mathrm{M}_p(m,1)$;

(ii) $\mathrm{M}_p(1,1,1) * \mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n}$;

(iii) $\mathrm{D}_8 * \mathrm{M}_2(m,1)$, $m \geqslant 3$;

(iv) $\mathrm{D}_8 * \mathrm{D}_8 * \mathrm{C}_{2^n}$;

(v) $\mathrm{D}_8 * \mathrm{D}_8 * \mathrm{Q}_8$;

(vi) $(\mathrm{D}_8 * \mathrm{Q}_8) \times \mathrm{C}_2$;

(vii) $(\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n}) \times \mathrm{C}_p$;

(viii) $(\mathrm{D}_8 * \mathrm{C}_{2^n}) \times \mathrm{C}_2$;

(ix) $\mathrm{M}_p(m,1) \times \mathrm{C}_p$, 当 $p=2$ 时, $m \geqslant 3$;

(x) $\mathrm{M}_p(2,1,1) * \mathrm{C}_{p^n}$, 其中 $\mathrm{M}_p(2,1,1) \bigcap \mathrm{C}_{p^n} = \mathrm{M}_p(2,1,1)'$;

(xi) $\mathrm{M}_2(2,1,1) * \mathrm{Q}_8$, 其中 $\mathrm{M}_2(2,1,1) \bigcap \mathrm{Q}_8 = \mathrm{M}_2(2,1,1)'$;

(xii) $\mathrm{Q}_8 \times \mathrm{C}_4$;

(xiii) $\mathrm{M}_p(m,2)$.

证明 $\Longrightarrow$: 因为 G 是非交换的, 则 G 至少有一个内交换子群. 检查定理 1.7.10 中的群可知, 非正规子群的阶至多为 p^2 的内交换群是

$$\mathrm{M}_p(m,2), \quad \mathrm{M}_p(m,1), \quad \mathrm{M}_p(2,1,1), \quad \mathrm{M}_p(1,1,1) \quad 和 \quad \mathrm{Q}_8.$$

情形 1 G 有子群 H 同构于 $\mathrm{M}_p(1,1,1)$ 或 D_8.

由引理 10.6.2 和引理 11.3.4 可得, $G = H * C_G(H)$, 其中 $C_G(H)$ 是 Dedekind 群或定理 11.1.7 列出的群之一.

若 $C_G(H)$ 是定理 11.1.7 列出的群之一, 易得 G 是群 (i) 到 (v) 之一.

设 $C_G(H)$ 是 Dedekind 群. 若 $C_G(H) \cong \mathrm{Q}_8 \times \mathrm{C}_2^k$, 则 $G \cong (\mathrm{D}_8 * \mathrm{Q}_8) \times \mathrm{C}_2^k$ 且易得 $k=1$, 即为群 (vi).

设 $C_G(H)$ 交换. 若 $C_G(H)$ 初等交换, 则 $G \cong H \times \mathrm{C}_p^k = (H * \mathrm{C}_p) \times \mathrm{C}_p^k$. 若 $C_G(H)$ 非初等交换, 取 $N \leqslant H$ 且 $N \ntrianglelefteq H$. 则对 $C_G(H)$ 中任意一个具有 $o(x) > p$ 的元素 x, 有 $|N\langle x\rangle| \geqslant p^3$, 因而 $N\langle x\rangle \trianglelefteq G$. 由命题 5.4.2 可知, $G' \leqslant N\langle x\rangle \bigcap C_G(H) = \langle x\rangle$. 于是 $C_G(H) \cong \mathrm{C}_{p^n} \times \mathrm{C}_p^k$ 且 $G \cong (H * \mathrm{C}_{p^n}) \times \mathrm{C}_p^k$, 其中 $n > 1$. 上述论证说明: 在任何情形下, $G \cong (H * \mathrm{C}_{p^n}) \times \mathrm{C}_p^k$, 其中 $n \geqslant 1$. 又由假设条件易得 $k=1$. 此时我们得到群 (vii) 或 (viii).

情形 2 G 无子群同构于 $\mathrm{M}_p(1,1,1)$ 或 D_8, 但有子群 H 同构于 $\mathrm{M}_p(m,1)$, 其中当 $p=2$ 时, $m \geqslant 3$.

由引理 10.6.2 和引理 11.3.4 可知, 我们仍然有 $G = H * C_G(H)$, 其中 $C_G(H)$ 是 Dedekind 群或定理 11.1.7 列出的群之一.

若后者发生, 不妨设 $G = M_1 * M_2$, $M_i = \langle a_i, b_i \mid a_i^{p^{m_i}} = b_i^p = 1, a_i^b = a_i^{1+p^{m_i-1}}\rangle$, $i = 1,2$, $m_1 \leqslant m_2$, 其中 $M_1 = H$, $M_2 = C_G(H)$. 设 $a_1^p = a_2^{sp}$. 令 $a_3 = a_1 a_2^{-s}$. 则 $a_3^p = 1$, $\langle a_3, b_1\rangle \cong \mathrm{M}_p(1,1,1)$, 矛盾. 于是 $C_G(H)$ 是 Dedekind 群. 若 $C_G(H) \cong \mathrm{Q}_8 \times \mathrm{C}_2^k$, 则 G 有子群同构于 $\mathrm{M}_p(m,1) * \mathrm{Q}_8$. 由命题 11.3.1 可知, G 有子群同构于 D_8, 矛盾. 故 $C_G(H)$ 交换. 与情形 1 的论证类似可得

$$G \cong (\mathrm{M}_p(m,1) * \mathrm{C}_{p^n}) \times \mathrm{C}_p^k,$$

其中 $n \geqslant 1$ 且 $k \leqslant 1$.

若 $\mathrm{C}_{p^n} \leqslant \mathrm{M}_p(m,1)$, 我们得到群 (ix).

若 $\mathrm{C}_{p^n} \nleqslant \mathrm{M}_p(m,1)$, 由定理 11.1.7 可知, $\mathrm{M}_p(m,1) * \mathrm{C}_{p^n}$ 有阶 $\geqslant p^2$ 的非正规子群. 因而 $k=0$ 且 $G \cong \mathrm{M}_p(m,1) * \mathrm{C}_{p^n}$. 由命题 11.3.2, 当 $m > n$ 时, 我们得到群 (ix). 当 $m \leqslant n$ 时, 我们得到群 (x). 反之, 当 $n \geqslant 2$ 时, 群 (ix) 和 (x) 满足情形 2 的假设.

情形 3　G 无子群同构于 $\mathrm{M}_p(1,1,1)$ 或 $\mathrm{M}_p(m,1)$, 但有子群 H 同构于 $\mathrm{M}_p(2,1,1)$.

由引理 10.6.2 可知, $G = H * C_G(H)$. 设

$$H = \langle a, b \mid a^{p^2} = b^p = c^p = 1, [a,b] = c, [c,a] = [c,b] = 1 \rangle \quad 且 \quad N \leqslant C_G(H).$$

若 $|N| \geqslant p^2$, 则 $|\langle b \rangle N| \geqslant p^3$. 因而 $\langle b \rangle N \trianglelefteq G$. 由命题 5.4.2 可得, $G' \leqslant \langle b \rangle N \bigcap C_G(H) = N$. 因而 $N \trianglelefteq G$. 若 $|N| = p$, 我们断言 $N \leqslant Z(G)$. 若否, $|\langle a \rangle N| \geqslant p^3$. 因而 $\langle a \rangle N \trianglelefteq G$. 再由命题 5.4.2 得, $G' \leqslant \langle a \rangle N \bigcap C_G(H) = \langle a^p \rangle N$. 因为 $|N| = p$ 且 $G' \bigcap \langle a \rangle = 1$, 故 $N \leqslant \langle a^p \rangle G' \leqslant Z(G)$, 矛盾. 这说明 $C_G(H)$ 是 Dedekind 群.

若 $C_G(H)$ 交换, 则对于 $C_G(H)$ 中任意一个 p 阶元 x, 与上面相同的论证可得 $x \in Z(G)$. 因为 $\mathrm{M}_p(2,1,1) \times \mathrm{C}_p$ 有一个 p^3 阶非正规子群, 故 $x \in H$. 因而对于 $C_G(H) \setminus H$ 任意元 y, 与上面相同的论证可得, $o(y) > p$ 且 $G' \leqslant \langle y \rangle$. 于是 $G = H * \mathrm{C}_{p^n}$. 若 $n \geqslant 2$, 由命题 11.3.2 可知, G 有一个子群同构于 $\mathrm{M}_p(m,1)$. 这与假设矛盾. 我们得到群 (x), 其中 $n = 1$.

若 $C_G(H) \cong \mathrm{Q}_8 \times \mathrm{C}_2^k$, 显然 $\mathrm{C}_2^k \leqslant H$. 我们得到群 (xi). 反之, $n=1$ 时的群 (x) 和群 (xi) 满足情形 3 的假设.

情形 4　G 无子群同构于 $\mathrm{M}_p(m,1)$ 或 $\mathrm{M}_p(2,1,1)$, 但有子群 H 同构于 Q_8.

由引理 10.6.2 得 $G = H * C_G(H)$. 因为 G 不是 Dedekind 群, 故 $\exp(C_G(H)) \geqslant 4$. 于是对于 $C_G(H) \setminus H$ 中任意一个阶 $\geqslant 4$ 的元 x, 由命题 11.3.1 可得 $H \bigcap \langle x \rangle = 1$. 因而 $G \cong \mathrm{Q}_8 \times A$, 其中 A 交换. 显然 A 必是 C_4. 我们得到群 (xii). 反之, 群 (xii) 满足情形 4 的假设.

情形 5　G 的所有内交换子群同构于 $\mathrm{M}_p(m,2)$.

由引理 10.6.2 可知, $G = H * C_G(H)$. 设

$$H = \langle a, b \mid a^{p^m} = b^{p^2} = 1, a^b = a^{1+p^{m-1}} \rangle.$$

若 $x \in G$ 但 $x \notin H$, 则 $|\langle b, x \rangle| \geqslant p^3$. 因而 $\langle b, x \rangle \trianglelefteq G$. 由命题 5.4.2 知, $G' \leqslant \langle b, x \rangle \bigcap C_G(H) = \langle b^p, x \rangle$. 这意味着存在整数 s, t 使得 $a^{p^{m-1}} = b^{sp} x^{tp}$. 若 $p \nmid s$, 则 $\langle a, b^s x^t \rangle$ 是有循环极大子群 $\langle a \rangle$ 的内交换群. 这与假设矛盾. 故 $G' \leqslant \langle x \rangle$. 假设 $a^{p^{m-i}} = x^{kp^{n-i}}$, 其中 $(k,p) = 1$, $|\langle a \rangle \bigcap \langle x \rangle| = p^i$, $i \geqslant 1$. 若 $m \leqslant n$, 则 $\langle a x^{-kp^{n-m}}, b \rangle \cong$

$\mathrm{M}_p(m-i,2,1)$. 矛盾. 若 $m>n$, 则 $\langle a^{p^{m-n}}x^{-k},b\rangle$ 是阶 $p^{m+2-i}\geqslant p^3$ 的非正规子群. 再一次矛盾. 这说明 $C_G(H)\leqslant H$. 我们得到群 (xiii). 反之, 群 (xiii) 满足情形 5 的假设.

$\Longleftarrow$: 我们证明定理 11.3.5 中的群互不同构. 由必要性的证明过程看出, 只需证在情形 1 中得到的群 (i)—(viii) 互不同构即可.

注意到对于群 (v), $d(G)=6$. 然而对于其他群, $d(G)\leqslant 5$. 另一方面, 群 (iii), (iv), (vi) 和 (viii) 是 2 群, 而群 (i), (ii) 和 (vii) 不是 2 群. 故我们只需分两种情形讨论.

对于群 (i) 和 (ii), $Z(G)$ 循环. 而对于群 (vii), $Z(G)$ 不循环. 对于群 (i), $d(G)=4$ 且 $\exp(G)>p$. 而对于群 (ii), $d(G)=5$ 或 $d(G)=4$ 且 $\exp(G)=p$. 因而群 (i), (ii) 和 (vii) 互不同构.

对于群 (iii) 和 (iv), $Z(G)$ 循环. 而对于群 (vi) 和 (viii), $Z(G)$ 不循环. 若群 (vi) 和 (viii) 的阶相同, 则 $n=3$. 然而对于群 (viii), $\exp(G)=8$. 对于群 (vi), $\exp(G)=4$. 若群 (iii) 和 (iv) 的阶相同, 则对于群 (iii), $d(G)=4$. 对于群 (iv), $d(G)=5$. 因而群 (iii), (iv), (vi) 和 (viii) 互不同构.

最后证明: 群 (i)—(xiii) 满足定理 11.3.5 的假设.

显而易见, 对于群 (i)—(xiii) 均有 $|G'|=p$. 由定理 11.1.7 可知, 对于群 (i)—(xiii) 均有一个阶 $\geqslant p^2$ 的非正规子群. 设 $N\leqslant G$ 且 $|N|\geqslant p^3$. 下证对于群 (i)—(xiii), $N\trianglelefteq G$. 若 $N\ntrianglelefteq G$, 则

(Ⅰ) 对于群 (i)—(ix), $\mho_1(G)$ 循环, 且当 $\mho_1(G)\neq 1$ 时, $G'\leqslant\mho(G)$. 因为 $N\ntrianglelefteq G$, 故 $G'\nleqslant N$. 于是 $N'=1$ 且 $\mho_1(N)=1$. 因而 N 初等交换. 简单验证可知, G 的不含 G' 的初等交换子群的阶 $\leqslant p^2$, 矛盾.

(Ⅱ) 对于群 (x) 和 (xiii), G 有一个循环子群 C 使得 $G'\leqslant C\leqslant Z(G)$ 且 $|G:C|=p^3$. 因为 $N\ntrianglelefteq G$, 故 $G'\nleqslant N$. 于是 $N\bigcap C=1$. 因而 $NC=G$, 故 $N\trianglelefteq G$, 矛盾.

(Ⅲ) 对于群 (xi) 和 (xii), 注意到 $\exp(G)=4=|\Omega_1(G)|$. 因为 $|N|\geqslant p^3$, 我们总有 $N\geqslant\Omega_1(G)\geqslant G'$, 矛盾. □

引理 11.3.6 设 $|G'|=p^2$. 若 $K\leqslant G'\bigcap Z(G)$, $|K|=p$, $G/K\cong \mathrm{D}_8*\mathrm{C}_{2^n}$, $\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^n}$ 或 $\mathrm{D}_8*\mathrm{Q}_8$, 其中 $n\geqslant 2$, 则 $G'\cong \mathrm{C}_p^2$, $n=2$, $\exp(G)=p^2$ 且 $G'\leqslant Z(G)$.

证明 由命题 11.3.2, 当 $\overline{G}=G/K\cong\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^n}$ 时, 可取 $H\leqslant G$ 使得 $\overline{H}=HK/K\cong\mathrm{M}_p(2,1)$. 另一方面, 当 $\overline{G}\cong\mathrm{D}_8*\mathrm{C}_{2^n}$ 或 $\mathrm{D}_8*\mathrm{Q}_8$ 时, 可取 H 使得 $\overline{H}\cong\mathrm{Q}_8$. 若 G' 循环, 由 $\overline{H}'=\overline{G}'$ 可得 $H'=G'$. 于是 H 是 p^4 阶群, $H'\cong\mathrm{C}_{p^2}$ 且 $H/\mho_1(H')\cong\mathrm{M}_p(2,1)$ 或 Q_8. 然而由 p^4 阶群的分类易知, 这样的群不存在. 因而 $G'\cong\mathrm{C}_p^2$.

若 $\overline{G} \cong \mathrm{D}_8 * \mathrm{C}_{2^n}$ 或 $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n}$, 断言 $n=2$: 取 $Z \leqslant G$ 使得 $Z/K = Z(\overline{G})$. 因为 $Z(\overline{G})$ 循环且 $G' \leqslant Z$, 其中 $C \cong \mathrm{C}_{2^n}$ 或 C_{p^n}, 有 $Z = K \times C$. 若 $n \geqslant 3$, 则 $G' \nleqslant C \trianglelefteq G$. 由命题 5.4.2 得 $C \leqslant Z(G)$. 于是 $|G:Z(G)| \leqslant |G:Z| = 4$ 或 p^2. 由此得出 $|G'| \leqslant p$, 矛盾.

现在我们总有 $\mho_1(G)K/K = \mho_1(G/K) = (G/K)' = G'/K'$. 因而 $\mho_1(G) \leqslant G'$, $\exp(G) = p^2$.

最后证明 $G' \leqslant Z(G)$. 若 $G/K \cong \mathrm{D}_8 * \mathrm{C}_4$ 或 $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^2}$, 则

$$G/K = \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^2} = \bar{b}^p = \bar{c}^p = \bar{1},\ [\bar{a}, \bar{b}] = [\bar{a}, \bar{c}] = \bar{1},\ [\bar{b}, \bar{c}] = \bar{a}^p \rangle.$$

于是 $G = \langle a, b, c \rangle$ 且 $G' = \langle a^p \rangle \times K$. 因为 $[a,b] \in K \leqslant Z(G)$, 故 $[a^p, b] = [a,b]^p = 1$. 类似地, $[a^p, c] = 1$. 因而 $G' \leqslant Z(G)$. 若 $G/K \cong \mathrm{D}_8 * \mathrm{Q}_8$, 则

$$\begin{aligned} G/K = \langle \bar{a}, \bar{b}, \bar{c}, \bar{d} \mid \bar{a}^4 = \bar{c}^2 = \bar{d}^2 = \bar{1},\ \ \bar{a}^2 = \bar{b}^2 = [\bar{a}, \bar{b}] = [\bar{c}, \bar{d}], \\ [\bar{a}, \bar{c}] = [\bar{a}, \bar{d}] = [\bar{b}, \bar{c}] = [\bar{b}, \bar{d}] = \bar{1} \rangle. \end{aligned}$$

由此得出 $[a^2, c] = [a^2, d] = [b^2, c] = [b^2, d] = 1$. 因而

$$G' = \langle a^2 \rangle \times K = \langle b^2 \rangle \times K \leqslant Z(G).$$ □

定理 11.3.7 *G 是具有 $|G'| = p^2$ 的 $\mathcal{N}_2$ 群当且仅当 G 同构于下列互不同构的群之一.*

(i) *p^4 阶的极大类群;*

(ii) $\langle a, b, c \mid a^4 = b^4 = c^2 = 1,\ [a,b] = 1,\ [a,c] = b^2,\ [b,c] = a^2 b^2 \rangle$;

(iii) $\langle a, b, c \mid a^4 = b^4 = 1,\ c^2 = b^2,\ [a,b] = 1,\ [a,c] = b^2,\ [b,c] = a^2 \rangle$;

(iv) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1,\ [a,b] = 1,\ [a,c] = b^p,\ [b,c] = a^p b^{wp} \rangle$, *其中 $w = 1, 2, \cdots, \dfrac{p-1}{2}$, $1 + \dfrac{w^2}{4}$ 模 p 不是一个平方数;*

(v) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1,\ [a,b] = 1,\ [a,c] = b^{\nu p},\ [b,c] = a^p b^{wp} \rangle$, *其中 ν 是模 p 的平方非剩余, $w = 0, 1, \cdots, \dfrac{p-1}{2}$, $\nu + \dfrac{w^2}{4}$ 模 p 不是一个平方数;*

(vi) $\langle a, b, c, d \mid a^4 = b^4 = 1,\ c^2 = a^2 b^2,\ d^2 = a^2,\ [a,b] = a^2,\ [c,d] = a^2 b^2,\ [a,c] = [b,d] = 1,\ [b,c] = [a,d] = b^2 \rangle$.

证明 $\Longrightarrow$: 由假设可知, $|G| \geqslant p^4$. 若 $|G| = p^4$, 由 p^4 阶群的分类易知, G 是极大类的, 即为群 (i). 不妨设 $|G| \geqslant p^5$. 由定理 11.1.7 和引理 11.1.2 可知, 存在 $K \trianglelefteq G$ 使得 $|G':K| = p$ 且 G/K 同构于下列群之一: $\mathrm{M}_p(m,1)$, $\mathrm{D}_8 * \mathrm{C}_{2^n}$, $p > 2$ 时的 $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n}$ 或 $\mathrm{D}_8 * \mathrm{Q}_8$, 其中 $m \geqslant 3$ 且 $n \geqslant 2$. 又由引理 11.3.6 可得, $n = 2$.

情形 1 $G/K \cong \mathrm{M}_p(m,1)$.

不妨设 $G/K=\langle \bar{a},\bar{b} \mid \bar{a}^{p^m}=\bar{b}^p=\bar{1},\ [\bar{a},\bar{b}]=\bar{a}^{p^{m-1}}\rangle$. 因为 $K\leqslant G'$, 故 $G=\langle a,b\rangle$. 进一步地, 因为 $m\geqslant 3$, 故 $o(a)\geqslant p^3$. 于是 $\langle a\rangle \trianglelefteq G$. 由此推出 G 亚循环且有一个循环的极大子群 $\langle a\rangle$. 然而由定理 1.9.1 可知, 没有这样的群 G 满足 $|G|\geqslant p^5$ 且 $|G'|=p^2$.

情形 2 $G/K\cong \mathrm{D}_8 * \mathrm{C}_4$.

不妨设 $G/K=\langle \bar{a},\bar{b},\bar{c} \mid \bar{a}^4=\bar{b}^2=\bar{c}^2=\bar{1},\ [\bar{b},\bar{c}]=\bar{a}^2,\ [\bar{a},\bar{b}]=[\bar{a},\bar{c}]=\bar{1}\rangle$. 因为 $K\leqslant G'$, 故 $G=\langle a,b,c\rangle$. 由引理 11.3.6 可知, $\exp(G)=4$, $G'=\langle a^2\rangle\times K\leqslant Z(G)$. 注意到 $|\langle b,c\rangle|\geqslant 8$. 我们有 $\langle b,c\rangle\trianglelefteq G$. 因为 $G=\langle b,c\rangle\langle a\rangle$, 故 $|\langle b,c\rangle|\geqslant 16$. 不妨设 $o(b)=4$. 因而 $K=\langle b^2\rangle$. 于是

$$G=\langle a,b,c \mid a^4=b^4=1,\ c^2=b^{2v},\ [b,c]=a^2b^{2k},\ [a,b]=b^{2s},\ [a,c]=b^{2t}\rangle,$$

其中 k,v,s,t 是 0 或 1, 且 $s\neq 1$ 或 $t\neq 1$.

若 $v=0$, 则 $\langle a,c\rangle\trianglelefteq G$, $b^2=[a,b]$ 或 $[a,c]$. 由此推出 $b^2\in\langle a,c\rangle$. 因而 $[a,c]\neq 1$, 即 $t=1$. 计算可得 $|\langle ab,c\rangle|\geqslant 8$. 因而 $\langle ab,c\rangle\trianglelefteq G$. 显然 $G'\leqslant\langle ab,c\rangle$. 因为 $G'\leqslant Z(G)$, 故 $[ab,c]\neq(ab)^2$. 再由计算可得 $s\neq k$. 若 $s=0$, 则 $k=1$. 此时得到群 (ii). 若 $s=1$, 则 $k=0$. 令 $b_1=abc$. 则 $b_1^2=b^2$, $[a,b_1]=1$, $[b_1,c]=a^2b^2$. 此时 G 同构于群 (ii).

设 $v=1$. 若 $t=0$, 则 $s=1$. 若 $k=1$, 令 $c'=abc$. 则 $c'^2=1$. 这归结为上段的情形. 不妨设 $k=0$. 令 $b_1=c$, $c_1=b$. 此时得到群 (iii). 若 $s=0$, 与情形 $t=0$ 的论证类似可得群 (iii). 若 $s=t=1$, 令 $c_1=abc$. 则 $\bar{c}_1^2=1$ 且 $[a,c_1]=1$. 这又归结为讨论过的情形.

情形 3 $G/K\cong \mathrm{M}_p(1,1,1)*\mathrm{C}_{p^2}$, $p>2$.

不妨设 $G/K=\langle \bar{a},\bar{b},\bar{c} \mid \bar{a}^{p^2}=\bar{b}^p=\bar{c}^p=1,\ [\bar{a},\bar{b}]=[\bar{a},\bar{c}]=\bar{1},\ [\bar{b},\bar{c}]=\bar{a}^p\rangle$. 由引理 11.3.6 可知, $\exp(G)=p^2$, $G'=\langle a^p\rangle\times K\leqslant Z(G)$. 因为 $p>2$, G 是 p 交换的. 类似于情形 2 的论证, 不妨设

$$G=\langle a,b,c \mid a^{p^2}=b^{p^2}=1, c^p=b^{kp},\ [a,b]=b^{sp},\ [a,c]=b^{tp},\ [b,c]=a^pb^{wp}\rangle,$$

其中 $0\leqslant k,s,t,w<p$. 用 cb^{-k} 替换 c 可设 $k=0$. 由 $\langle a,c\rangle\trianglelefteq G$ 推出 $G'\leqslant\langle a,c\rangle$. 因而 $t\neq 0$. 用 $c^{-is}b$ 替换 b, 其中 $it\equiv 1(\mathrm{mod}\ p)$, 有 $s=0$.

对某个 i, 若 $t\equiv i^2(\mathrm{mod}\ p)$, 则用 a^j 替换 a, 用 c^j 替换 c, 其中 $ij\equiv 1(\mathrm{mod}\ p)$, 我们有 $t=1$. 再用 a^{-1} 替换 a, 用 c^{-1} 替换 c, 又由 $[b,c]=a^pb^{(p-w)p}$. 于是不妨设 $w\leqslant\dfrac{p-1}{2}$. 断言 $1+\dfrac{w^2}{4}$ 模 p 不是一个平方数. 若否, 设对某个 i, $1+\dfrac{w^2}{4}\equiv i^2(\mathrm{mod}\ p)$. 令 $j=i-\dfrac{w}{2}$ 且 $H=\langle a^jb,c^j\rangle$. 则 H 是 p^3 阶正规子群. 与假设矛盾. 此时得到群 (iv).

若 t 模 p 不是平方数, 取 ν 是模 p 的平方非剩余, 则存在 i 使得 $t = i^2\nu$. 用 a^j 替换 a, 用 c^j 替换 c, 其中 $ij \equiv 1 (\mathrm{mod}\ p)$, 则 $t = \nu$. 类似于上面的论证, 得到群 (v).

情形 4 $G/K \cong \mathrm{D}_8 * \mathrm{Q}_8$.

不妨设

$$G/K = \langle \bar{a}, \bar{b}, \bar{c}, \bar{d} \mid \bar{a}^4 = \bar{b}^2 = \bar{1},\ [\bar{a}, \bar{b}] = \bar{a}^2,\ \bar{c}^2 = \bar{d}^2 = \bar{a}^2,$$
$$[\bar{c}, \bar{d}] = \bar{a}^2,\ [\bar{a}, \bar{c}] = [\bar{a}, \bar{d}] = [\bar{b}, \bar{c}] = [\bar{b}, \bar{d}] = \bar{1} \rangle.$$

因为 $K \leqslant G'$, 故 $G = \langle a, b, c, d \rangle$. 由引理 11.3.6 可知, $\exp(G) = 4$, $G' = \langle a^2 \rangle \times K \leqslant Z(G)$. 设 $H/K = \overline{H} \leqslant \overline{G} = G/K$. 则可证下列事实:

若 $\overline{H} = \langle \bar{x}, \bar{y} \mid \bar{x}^4 = \bar{y}^2 = 1, \bar{x}^{\bar{y}} = \bar{x}^{-1} \rangle \cong \mathrm{D}_8$, 则 $o(y) = 4$. 因而 $H \cong \mathrm{M}_p(2,2)$. 事实上, 由引理 10.6.2 可知, $\overline{G} = \overline{H} * C_{\overline{G}}(\overline{H})$. 因而不妨设 $x = a$, $y = b$. 注意到 $C_{\langle c,d \rangle}(b) \neq 1$. 还可设 $[b, c] = 1$. 由定理的假设可得, $\langle b, c \rangle \trianglelefteq G$ 且 $\langle a, b \rangle \trianglelefteq G$. 若 $b^2 = 1$, 则

$$[\langle b, c \rangle, \langle a, d \rangle] \leqslant \langle b, c \rangle \bigcap G' = \langle c^2 \rangle \quad 且 \quad [\langle a, b \rangle, \langle c, d \rangle] \leqslant K \bigcap \langle a, b \rangle = 1.$$

因而 $G' = \langle c^2 \rangle$. 这与 $|G'| = p^2$ 矛盾. 于是 $o(b) = 4$, $K = \langle b^2 \rangle$. 进一步地, $\langle \bar{a}, \overline{ab} \rangle \cong \mathrm{D}_8$. 因而 $(ab)^2 = a^2b^2[a, b] \neq 1$. 于是 $[a, b] = a^2$, $H \cong \mathrm{M}_p(2, 2)$.

注意到 $C_{\langle c,d \rangle}(a) \neq 1$. 不妨设 $[a, c] = 1$. 令 $\overline{H_1} = \langle \overline{ca}, \bar{d} \rangle \cong \mathrm{D}_8$. 由上面证得的事实, 有 $(ca)^2 = c^2a^2[a, c] = c^2a^2 \neq 1$. 因而 $c^2 = a^2b^2$. 进一步地, $d^2 = [ca, d] = [c, d][a, d]$. 从而 $[c, d] = d^2[a, d]$. 令 $\overline{H_2} = \langle \overline{da}, \bar{c} \rangle \cong \mathrm{D}_8$. 同样的论证可得, $(da)^2 = d^2a^2[a, d] \neq 1$, $d^2[a, d] = a^2b^2$. 因而 $[c, d] = c^2 = a^2b^2$.

若 $d^2 = c^2$, 则

$$[\langle b \rangle, \langle c, d \rangle] \leqslant \langle c, d \rangle \bigcap K = 1, \quad (bc)^2 = b^2c^2 = a^2, \quad [d, c] = [d, bc] \in \langle a, bc \rangle \bigcap G' = \langle a^2 \rangle.$$

与 $[c, d] = a^2b^2$ 矛盾. 因而 $d^2 = a^2$. 故 $[a, d] = d^2[c, d] = b^2$.

若 $[b, c] = 1$, 则 $[a, d] \in \langle a, bc \rangle \bigcap G' = \langle a^2 \rangle$, 与 $[a, d] = b^2$ 矛盾. 因而 $[b, c] = b^2$.

若 $[b, d] = b^2$, 令 $d_1 = cd$, 则

$$d_1^2 = d^2, \quad [a, d_1] = [a, d], \quad [c, d_1] = [c, d], \quad [b, d_1] = 1.$$

于是可设 $[b, d] = 1$. 从而得到群 (vi).

$\Longleftarrow$: 首先证明定理中的群互不同构. 只需证群 (ii)—(v) 互不同构即可.

对于群 (ii) 和 (iii), 注意到 (ii) 和 (iii) 有一个极大子群 H 同构于 $\mathrm{C}_4 \times \mathrm{C}_4$. 然而, 对于 (ii), $G \setminus H$ 有一个对合, 而对于 (iii), $G \setminus H$ 没有一个对合.

对于群 (iv) 和 (v), 其阶为 $p^5(p>2)$. 首先证在同一类型的群中, 不同的参数对应不同构的群. 显然, $Z(G)=G'$. 因而 $\langle a,b\rangle$ 是 G 的唯一的交换极大子群.

对于群 (iv), 设具有参数 w_1 的群同构于具有参数 w_2 的群. 因为 $\langle a,b\rangle$ char G, 不妨设

$$a_2=a_1^{i_1}b_1^{j_1},\quad b_2=a_1^{i_2}b_1^{j_2},\quad c_2=a_1^{i_3}b_1^{j_3}c_1^k$$

满足

$$a_i^{p^2}=b_i^{p^2}=c_i^p=1,\quad [a_i,b_i]=1,\quad [a_i,c_i]=b_i^p,\quad [b_i,c_i]=a_i^pb_i^{w_ip},$$

其中 $i=1,2$, $\begin{vmatrix} i_1 & j_1 \\ i_2 & j_2 \end{vmatrix}\not\equiv 0(\text{mod }p)$ 且 $p\nmid k$. 因为

$$(a_1^{i_2}b_1^{j_2})^p=b_2^p=[a_2,c_2]=[a_1^{i_1}b_1^{j_1},a_1^{i_3}b_1^{j_3}c_1^k],$$

有

$$(1)\ \ j_1k\equiv i_2(\text{mod }p),\quad (2)\ i_1k+w_1j_1k\equiv j_2(\text{mod }p).$$

因为 $(a_1^{i_1}b_1^{j_1})^p(a_1^{i_2}b_1^{j_2})^{w_2p}=a_2^pb_2^{w_2p}=[b_2,c_2]=[a_1^{i_2}b_1^{j_2},a_1^{i_3}b_1^{j_3}c_1^k]$, 有

$$(3)\ \ j_2k\equiv i_1+w_2i_2(\text{mod }p),\quad (4)\ i_2k+w_1j_2k\equiv j_1+w_2j_2(\text{mod }p).$$

由 (1) 和 (4) 可得, $j_1(k^2-1)+j_2(kw_1-w_2)\equiv 0(\text{mod }p)$. 由 (1)—(3) 可得, $i_1(k^2-1)+i_2(kw_1-w_2)\equiv 0(\text{mod }p)$. 因为 $\begin{vmatrix} i_1 & j_1 \\ i_2 & j_2 \end{vmatrix}\not\equiv 0(\text{mod }p)$, 故 $k^2-1\equiv 0(\text{mod }p)$, $kw_1-w_2\equiv 0(\text{mod }p)$. 因为 $1\leqslant w_i\leqslant \dfrac{p-1}{2}$, 故 $w_1=w_2$.

类似可证, 群 (v) 中不同参数对应不同构的群.

其次证明, (iv) 和 (v) 不同构. 假设具有参数 w_1 的群 (iv) 与具有参数 w_2 的群 (v) 同构. 不妨设

$$a_2=a_1^{i_1}b_1^{j_1},\quad b_2=a_1^{i_2}b_1^{j_2},\quad c_2=a_1^{i_3}b_1^{j_3}c_1^k$$

满足

$$a_i^{p^2}=b_i^{p^2}=c_i^p=1,\quad [a_i,b_i]=1,\quad [a_1,c_1]=b_1^p,\quad [a_2,c_2]=b_2^{\nu p},\quad [b_i,c_i]=a_i^pb_i^{w_ip},$$

其中 $i=1,2$, $\begin{vmatrix} i_1 & j_1 \\ i_2 & j_2 \end{vmatrix}\not\equiv 0(\text{mod }p)$ 且 $p\nmid k$. 类似于上面的计算可得, $j_1(k^2\nu^{-1}-1)+j_2(kw_1-w_2)\equiv 0(\text{mod }p)$ 且 $i_1(k^2\nu^{-1}-1)+i_2(kw_1-w_2)\equiv 0(\text{mod }p)$. 因而 $\nu\equiv k^2(\text{mod }p)$, 矛盾.

最后证明定理中的群 (i)—(vi) 满足假设. 对于群 (i)—(vi), 显然 $|G'| = p^2$. 群 (i) 显然满足定理的假设.

对于 (ii)—(v), 均有 $|G| = p^5$. 首先证明, 对于 G' 的任意一个 p 阶子群 K, $\overline{G} = G/K$ 是 Dedekind 群或列在定理 11.1.7 中的群之一. 易证群 (ii) 具有 $\overline{G} \cong \mathrm{D}_8 * \mathrm{C}_4$, 群 (iii) 具有 $\overline{G} \cong \mathrm{D}_8 * \mathrm{C}_4$ 或 $\mathrm{Q}_8 \times \mathrm{C}_2$. 群 (iv) 和 (v), $G/\langle b^p\rangle \cong \mathrm{M}_p(1,1,1) * \mathrm{C}_{p^2}$. 故可设 $K = \langle a^p b^{xp}\rangle$. 令 $\overline{M} = \langle \bar{a}\bar{b}^x, \bar{c}\rangle$. 注意到 $(\bar{a}\bar{b}^x)^p = \bar{c}^p = \bar{1}$, $[\bar{a}\bar{b}^x, \bar{c}] = \bar{b}^{p(\nu^i - x^2 + xw)}$, 其中对于 (iv), $i = 0$. 而对于 (v), $i = 1$. 因为 $\nu^i - x^2 + xw = \nu^i + \dfrac{w}{4} - \left(x - \dfrac{w}{2}\right)^2 \neq 0 \pmod p$, 故 $M \cong \mathrm{M}_p(1,1,1)$. 注意到 $|\overline{G}'| = p$ 且 $\exp(\overline{G}) = p^2$. 由引理 10.6.2 可得, $\overline{G} \cong \mathrm{M}_p(1,1,1) * \mathrm{C}_{p^2}$.

现在只需证 G 的所有 p^3 阶子群均正规即可. 设 $H \leqslant G$, $|H| = p^3$ 且 $H \ntrianglelefteq G$. 则 $G' \nleqslant H$. 注意到 $G' = Z(G)$ 的阶为 p^2. 若 $H \bigcap G' = 1$, 则 $G = G' \times H$. 这与 $H \ntrianglelefteq G$ 矛盾. 因而 $|H \bigcap G'| = p$. 于是 $G/H \bigcap G'$ 是 Dedekind 群或列在定理 11.1.7 中的群之一. 故 $H/H \bigcap G' \trianglelefteq G/H \bigcap G'$, 因而 $H \trianglelefteq G$, 又是矛盾.

对于群 (vi), 计算可得: $\Omega_1(G) = Z(G) = G' = \langle a^2\rangle \times \langle b^2\rangle$. 设 H 是 G 的非正规子群. 则 $|H \bigcap G'| \leqslant 2$. 因为 $H \bigcap \Omega_1(G) = \Omega_1(H)$, 故 H 有唯一的 2 阶元. 由此推出 H 是循环群或四元数群. 若 $|H| \geqslant 8$, 则 H 是四元数群. 取 $K \leqslant G'$ 且 $K \neq H'$. 令 $\overline{G} = G/K$. 因为 $\overline{H} = HK/K \cong \mathrm{Q}_8$ 且 $|\overline{G}'| = 2$, 由引理 10.6.2 知, $\overline{G} = \overline{H} * C_{\overline{G}}(\overline{H})$. 令 $C/K = C_{\overline{G}}(\overline{H})$. 则 $G = HC$, $H \bigcap C = H'$. 因而 G/H' 是 8 阶的初等交换群. 然而, 对于 $1 < K < G'$, $G/K \cong \mathrm{D}_8 * \mathrm{Q}_8$ 及 $\mathrm{D}_8 * \mathrm{Q}_8$ 无 8 阶的初等交换子群, 矛盾. □

综上所述, 我们有下述结果.

定理 11.3.8　设 G 是有限 p 群. 则 G 的阶 $\geqslant p^3$ 的子群均正规当且仅当 G 是 Dedekind 群或是定理 11.1.7、定理 11.3.5 和定理 11.3.7 中的群之一.

对于有限非素数幂阶的群、非正规子群的阶为素数 p 或 pq 的有限群以及非正规子群均循环的有限群的结构已被确定. 鉴于篇幅所限, 这里只列出结果, 其证明参看文献 [275].

设 G 是有限群, $|G| = \prod\limits_{i=1}^{s} p_i^{k_i}$, 其中 p_i 是素数, $i = 1, 2, \cdots, s$, 当 $i \neq j$ 时, $p_i \neq p_j$. 记 $w(G) = \sum\limits_{i=1}^{s} k_i$.

定理 11.3.9　设 G 是幂零群但不是素数幂阶群. 若 G 的满足 $w(H) \geqslant 3$ 的子群 H 均正规, 则 G 是 Dedekind 群或 $G = P \times H$, 其中 $P \in \mathrm{Syl}_p(G)$ 且 P 是定理 11.1.7 中的群之一, $H \cong \mathrm{C}_q$, 其中 $q (\neq p)$ 是素数.

定理 11.3.10　设 G 是非幂零群, p, q, r 是素数 (可以相同). 若 G 的满足 $w(H) \geqslant 3$ 的子群 H 均正规, 则 G 是下列群之一.

(i) 满足 $w(G) \leqslant 3$ 的非幂零群;

(ii) $H \times \mathrm{C}_p$, 其中 H 是阶为 p^2q 的内幂零群;

(iii) 阶为 p^3q 的内幂零群;

(iv) $P \rtimes \mathrm{C}_q$, 其中 P 是 p^3 阶群, $G/\Omega_1(\Phi(P))$ 是阶为 p^2q 的内幂零群;

(v) $\mathrm{C}_p^2 \rtimes H$, 其中 $|H| = qr$ 且 H 不可约地作用在 C_p^2 上;

(vi) $\mathrm{C}_p^3 \rtimes H$, 其中 $|H| = qr$ 且 H 不可约地作用在 C_p^3 上.

定理 11.3.11 设 G 是非幂零群. 若 G 的非正规子群均循环, 则 G 是下列群之一.

(i) $\mathrm{C}_p \rtimes \mathrm{C}_n$, 其中 p 是素数;

(ii) $\mathrm{C}_p^2 \rtimes \mathrm{C}_n$, 其中 p 是素数, $(p, n) = 1$, C_n 不可约地作用在 C_p^2 上;

(iii)$(\mathrm{Q}_8 \rtimes \mathrm{C}_{3^m}) \times \mathrm{C}_n$, 其中 $(2, n) = (3, n) = 1$.

推论 11.3.12 设 G 是非幂零群. 若 G 的非正规子群的阶均为素数, 则 G 是阶为 pq 或 p^2q 的内幂零群.

11.4 非正规子群的阶至多为 p^3 的 p 群

非正规子群的阶至多为 p^3 的有限 p 群的分类已由张勤海等在文献 [278], [279] 完成. 本节分 $p \neq 2$ 和 $p = 2$ 两种情形介绍这项分类工作.

为叙述简便, 以下我们假设所讨论的 p 群 G 满足: G 的阶 $\geqslant p^4$ 的子群均正规且 G 至少有一个 p^3 阶非正规子群. 记这样的群为 $\mathcal{N}_3$ 群. $\mu(G)$ 表示 G 的非正规子群阶的极大值. 不失一般性, 本节总假设 $|G| \geqslant p^6$.

引理 11.4.1 设 G 是有限 p 群, $\mu(G) = |G'| = p^k$, 其中 $k \geqslant 2$. 若 $N \leqslant G'$, $N \trianglelefteq G$ 且 $|N| = p$, 则 $\mu(G/N) = p^{k-1}$.

证明 设 $H/N \leqslant G/N$ 且 $|H/N| \geqslant p^k$. 则 $|H| \geqslant p^{k+1}$. 因为 $\mu(G) = p^k$, 故 $H \trianglelefteq G$. 因而 $H/N \trianglelefteq G/N$. 由此推出 $\mu(G/N) \leqslant p^{k-1}$. 由 [181] 中的定理 2.3 可知, $p^{k-1} = |G'/N| = |(G/N)'| \leqslant \mu(G/N)$. 因而 $\mu(G/N) = p^{k-1}$. □

先看 $p \neq 2$ 的情形.

引理 11.4.2 设 G 是有限 p 群且 $\mu(G) = p^3$. 则

(1) $|G'| \leqslant p^2$;

(2) 若 $|G'| = p^2$, 则 $d(G) \leqslant 5$.

证明 (1) 由 [181] 中的定理 2.3 可知, $|G'| \leqslant p^3$. 下证 $|G'| \leqslant p^2$. 若否, 则 $|G'| = p^3$. 于是存在 $N \leqslant G'$ 满足 $|N| = p$ 且 $N \trianglelefteq G$ 使得 $|(G/N)'| = |G'/N| = p^2$. 因为 $\mu(G) = p^3$, 由引理 11.4.1 可得 $\mu(G/N) = p^2$. 于是 G/N 是定理 11.3.7 中的群之一. 因为 $p > 2$, 故 G/N 是定理 11.3.7 中的群 (iv) 或 (v). 不妨设

$$G/N \cong \langle \overline{a}, \overline{b}, \overline{c} \mid \overline{a}^{p^2} = \overline{b}^{p^2} = \overline{c}^p = 1, [\overline{a}, \overline{b}] = 1, [\overline{a}, \overline{c}] = \overline{b}^{\nu p}, [\overline{b}, \overline{c}] = \overline{a}^p \overline{b}^{wp} \rangle,$$

其中当 ν 是模 p 的平方非剩余时, $w=0,1,\cdots,\dfrac{p-1}{2}$; 当 $\nu=1$ 时, $w=1,\cdots,\dfrac{p-1}{2}$ 且 $\nu+\dfrac{w^2}{4}$.

为方便令 $N=\langle x\rangle$. 则可设

$$G=\langle a,b,c,x\mid a^{p^2}=x^{i_1},b^{p^2}=x^{i_2},c^p=x^{i_3},[a,b]=x^{i_4},[a,c]=b^{\nu p}x^{i_5},$$
$$[b,c]=a^pb^{wp}x^{i_6},x^p=1,[x,a]=[x,b]=[x,c]=1\rangle,\quad \text{其中}\quad 0\leqslant i_k\leqslant p-1.$$

因为 $G/N=\langle\bar a,\bar b\rangle$, 故 $G'=\langle a^p,b^p,x\rangle$. 又因为 $[a,b]=x^{i_4}$, 故 $[a,b^p]=[a^p,b]=1$. 由此可得 $[a^p,b^p]=1$, 即 G' 交换. 于是 G 亚交换. 由命题 1.1.9 可知,

$$[a,c^p]=[a,c]^{\binom{p}{1}}[a,c,c]^{\binom{p}{2}}=[a,c]^p=b^{\nu p^2}.$$

另一方面, 由 $c^p=x^{i_3}$ 推出 $[a,c^p]=1$. 因而 $b^{p^2}=1$. 类似地, 计算 $[b,c^p]$ 可得 $a^{p^2}=1$.

因为 $|G'|=p^3$, 故 $i_4\neq 0$. 设 $i_3=0$. 因为 $|\langle a,c\rangle|\geqslant p^4$, 故 $\langle a,c\rangle\trianglelefteq G$. 另一方面, $[a,b]=x^{i_4}\notin\langle a,c\rangle$. 矛盾. 于是 $i_3\neq 0$. 则

$$G=\langle a,b,c\mid a^{p^2}=b^{p^2}=c^{p^2}=1,[a,b]=c^{pi_4},[a,c]=b^{\nu p}c^{pi_5},[b,c]=a^pb^{pw}c^{pi_6}\rangle.$$

明显地, $|G|=p^6$ 且 $G'=\langle a^p,\ b^p,\ c^p\rangle\leqslant Z(G)$. 设 H 是 G 的 p^4 阶子群. 则 $H\trianglelefteq G$ 且 $|G/H|=p^2$. 于是 G/H 交换. 由此推出 $G'\leqslant H$. 因为 $G'\leqslant Z(G)$, 故 H 交换. 又 $|G'|=p^3$, 由定理 1.7.7 可知 G 不是 $\mathcal{A}_1$ 群. 于是 G 是 $\mathcal{A}_2$ 群. 然而, 检查定理 9.3.1 中的群, 或由推论 9.3.2 可知, 不存在这样的群, 矛盾.

(2) 若 $|G'|=p^2$, 则存在 $N\leqslant G'$ 满足 $|N|=p$ 且 $N\trianglelefteq G$ 使得 $|(G/N)'|=|G'/N|=p$. 因为 $\mu(G)=p^3$, 故 $\mu(G/N)\leqslant p^2$. 于是 G/N 是定理 11.1.7 和定理 11.3.5 中的群之一. 因为 $N\leqslant G'$, 故 $d(G)=d(G/N)$. 由定理 11.1.7 和定理 11.3.5 看出 $d(G)\leqslant 5$. □

定理 11.4.3 *设 G 是有限 p 群, $d(G)=2$ 且 $|G'|=p^2$. 则 $\mu(G)=p^3$ 当且仅当 $G\cong\langle a,b\mid a^{p^n}=b^{p^2}=1,[a,b]=a^{p^{n-2}}\rangle$, 其中 $n\geqslant 4$. 进一步地, $Z(G)=\langle a^{p^2}\rangle$, $G'=\langle a^{p^{n-2}}\rangle$, G 亚循环且 G 无交换极大子群.*

证明 因为 $|G'|=p^2$, 故存在 $N\leqslant G'$ 满足 $|N|=p$ 且 $N\trianglelefteq G$ 使得 $|(G/N)'|=|G'/N|=p$. 又 $\mu(G)=p^3$, 故 $\mu(G/N)\leqslant p^2$. 于是 G/N 是定理 11.1.7 和定理 11.3.5 中的群之一. 因为 $d(G)=2$ 且 $N\leqslant G'$, 故 $d(G/N)=2$. 又 $|G|\geqslant p^6$ 且 $|N|=p$, 故 $|G/N|\geqslant p^5$. 由定理 1.7.7 和定理 1.7.10 可得, $G/N\cong \mathrm{M}_p(m,1)$ 或 $\mathrm{M}_p(m,2)$. 为方便, 设 $\overline{G}=G/N$, $N=\langle x\rangle$.

若 $\overline{G}\cong\mathrm{M}_p(m,1)=\langle\overline{a},\overline{b}\mid\overline{a}^{p^m}=\overline{b}^p=\overline{1},[\overline{a},\overline{b}]=\overline{a}^{p^{m-1}}\rangle$, 则

$$G=\langle a,b\mid a^{p^m}=x^{i_1},b^p=x^{i_2},x^p=1,[a,b]=a^{p^{m-1}}x^{i_3},[a,x]=[b,x]=1\rangle,$$

其中 $i_1, i_2, i_3 \in \{1, \cdots, p\}$. 由 [24] 中的定理 2 可知, G 亚循环. 于是 $G' = \langle a^{p^{m-1}}, x\rangle$ 循环. 由此可知, $\langle a^{p^m}\rangle = \langle x\rangle$ 且 $\langle a\rangle$ 是 G 的循环极大子群. 由定理 1.9.1 可知, $G \cong \mathrm{M}_p(m+1,1)$ 且 $|G'| = p$. 与 $|G'| = p^2$ 矛盾.

若 $\overline{G} \cong \mathrm{M}_p(m,2)= \langle \overline{a}, \overline{b} \mid \overline{a}^{p^m} = \overline{b}^{p^2} = \overline{1}, [\overline{a}, \overline{b}] = \overline{a}^{p^{m-1}}\rangle$, 则

$$G = \langle a, b \mid a^{p^m} = x^{i_1}, b^{p^2} = x^{i_2}, x^p = 1, [a,b] = a^{p^{m-1}} x^{i_3}, [a,x] = [b,x] = 1\rangle,$$

其中 $i_1, i_2, i_3 \in \{1, \cdots, p\}$. 由 [24] 中的定理 2 可知, G 亚循环. 于是 $G' = \langle a^{p^{m-1}}, x\rangle$ 循环. 由此推出 $\langle a^{p^m}\rangle = \langle x\rangle$. 于是

$$G = \langle a, b \mid a^{p^{m+1}} = 1, b^{p^2} = a^{i_2 p^m}, [a,b] = a^{(1+pi_3)p^{m-1}}\rangle.$$

令 $a_1 = a^{1+pi_3}$ 且 $b_1 = (ba^{-i_2 p^{m-2}})^{1-pi_3}$. 则

$$a_1^{p^m} = a^{p^m}, \quad b_1^{p^2} = (ba^{-i_2 p^{m-2}})^{p^2} = b^{p^2}(a^{-i_2 p^{m-2}})^{p^2} = b^{p^2} a^{-i_2 p^m} = 1,$$

且

$$[a_1, b_1] = [a,b][a,b]^{pi_3}[a,b]^{-pi_3}[a,b]^{-(pi_3)^2} = [a,b] = a_1^{p^{m-1}}.$$

于是

$$G = \langle a, b \mid a^{p^{m+1}} = 1, b^{p^2} = a^{i_2 p^m}, [a,b] = a^{p^{m-1}}\rangle.$$

用 $ba^{-i_2 p^{m-2}}$ 替换 b 可得, $b^{p^2} = 1$. 于是

$$G = \langle a, b \mid a^{p^m} = b^{p^2} = 1, [a,b] = a^{p^{m-2}}\rangle.$$

此为定理中的群.

反之, $\langle a^{p^{m-1}}, b\rangle$ 是 G 的 p^3 阶的非正规子群. 即 $\mu(G) \geqslant p^3$. 设 $H \leqslant G$ 且 $|H| \geqslant p^4$. 断言 $|H \bigcap \langle a\rangle| \geqslant p^2$. 若否, 则 $|H \bigcap \langle a\rangle| \leqslant p$. 因为 $G' \leqslant \langle a\rangle \trianglelefteq G$, 故 $\langle a\rangle H \leqslant G$. 另一方面,

$$|\langle a\rangle H| = \frac{|H||\langle a\rangle|}{|H \bigcap \langle a\rangle|} \geqslant \frac{p^{4+m}}{p} = p^{m+3} > p^{m+2} = |G|.$$

矛盾. 于是 $G' = \langle a^{p^{m-2}}\rangle \leqslant H$. 因而 $H \trianglelefteq G$. 这说明 $\mu(G) = p^3$. □

引理 11.4.4 设 G 是有限 p 群, $\mu(G) = p^3$. 若 $d(G) \geqslant 3$ 且 $|G'| = p^2$, 则 $G' \cong \mathrm{C}_p^2$ 且 $c(G) = 2$.

证明 设 G 是反例. 则存在 $H \leqslant G$ 使得 $d(H) = 2$ 且 $H' = G'$. 令 H 的阶极大. 因为 $d(G) \geqslant 3$, 故 $H < G$. 然而, 由定理 11.3.7 可知, 不存在这样的 H 满足 $|H'| = p^2$, $d(H) = 2$ 且 $\mu(H) = p^2$. 因为 $\mu(H) \leqslant \mu(G)$, 故 $\mu(H) = p^3$. 由定理 11.4.3 就有

$$H = \langle x, y \mid x^{p^n} = y^{p^2} = 1, [x,y] = x^{p^{n-2}}\rangle,$$

其中 $n \geqslant 3$. 因为 $H' = G'$, 故 $H \lhd G$. 取 $d \in G \backslash H$. 令 $L = H\langle d \rangle$. 由 H 阶的极大性即得 $d(L) = 3$. 令 $N = \Omega_1(H')$. 则 $N = \langle x^{p^{n-1}} \rangle$ 且 $N \lhd L$. 由引理 11.4.1 可得, $\mu(L/N) = p^2$. 注意到 $H/N \cong \mathrm{M}_p(n-1, 2) \leqslant L/N$. 由定理 11.1.7, 定理 11.3.5 和定理 11.3.7 可知, $L/N \cong \mathrm{M}_p(2,1,1) * \mathrm{C}_{p^{n-1}}$. 不妨设

$$L/N = \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^2} = \bar{b}^p = \bar{c}^{p^{n-1}} = \bar{1}, [\bar{a}, \bar{b}] = \bar{c}^{p^{n-2}}, [\bar{c}, \bar{a}] = [\bar{c}, \bar{b}] = \bar{1} \rangle.$$

于是 $L' = H' = \langle x^{p^{n-1}}, c^{p^{n-2}} \rangle$. 因为 $[a, c] \in N \leqslant Z(L)$, 故 $[a, c^{p^{n-2}}] = [a, c]^{p^{n-2}} = 1$. 同理, $[b, c^{p^{n-2}}] = 1$. 因而 $c^{p^{n-2}} \in Z(L)$. 进一步地, $L' \leqslant Z(L)$. 又 $b^p \in N \leqslant Z(L)$, 故 $1 = [a, b^p] = [a, b]^p = c^{p^{n-1}}$. 由此推出 $\exp(L') = p$. 于是 $G' = L' \cong \mathrm{C}_p \times \mathrm{C}_p$. 因为 G 是反例, 故 $c(G) = 3$. 于是存在 $d_1 \in G$ 使得 $[H', d_1] \neq 1$. 令 $L_1 = H\langle d_1 \rangle$. 由对 L 相同的论证可知, $L_1' \leqslant Z(L_1)$. 由此推出 $[H', d_1] \leqslant (L_1)_3 = 1$. 矛盾. □

定理 11.4.5 设 G 是有限 p 群, $d(G) = 3$ 且 $|G'| = p^2$. 则 $\mu(G) = p^3$ 当且仅当 G 是下列互不同构的群之一.

(1a) $G = \langle a, b, c \mid a^p = b^{p^3} = c^{p^3} = 1, [b, c] = 1, [c, a] = b^{p^2} c^{tp^2}, [a, b] = b^{-tp^2} c^{\nu p^2} \rangle = (\langle b \rangle \times \langle c \rangle) \rtimes \langle a \rangle$, 其中当 -1 是模 p 的平方非剩余时, $\nu = 1$; 当 -1 是模 p 的平方剩余时, ν 是模 p 的平方非剩余; $t \in \left\{0, 1, \cdots, \dfrac{p-1}{2}\right\}$. 进一步地, $|G| = p^7$, $Z(G) = \Phi(G) = \langle b^p, c^p \rangle, G' = \langle b^{p^2}, c^{p^2} \rangle$.

(1b) $G = \langle a, b, c \mid a^{p^2} = b^{p^2} = c^{p^2} = 1, [b, c] = 1, [c, a] = b^p c^{tp}, [a, b] = b^{-tp} c^{\nu p} \rangle = (\langle b \rangle \times \langle c \rangle) \rtimes \langle a \rangle$, 其中当 -1 是模 p 的平方非剩余时, $\nu = 1$; 当 -1 是模 p 的平方剩余时, ν 是模 p 的平方非剩余; $t \in \left\{0, 1, \cdots, \dfrac{p-1}{2}\right\}$, 进一步地, $|G| = p^6$, $Z(G) = \Phi(G) = \langle a^p, b^p, c^p \rangle, G' = \langle b^p, c^p \rangle$.

(2) $G = \langle a, b, c \mid a^p = b^{p^3} = c^{p^2} = 1, [b, c] = 1, [c, a] = b^{p^2}, [a, b] = c^{\nu p} \rangle = (\langle b \rangle \times \langle c \rangle) \rtimes \langle a \rangle$, 其中 $\nu = 1$ 或是模 p 的平方非剩余, 进一步地, $|G| = p^6$, $Z(G) = \Phi(G) = \langle b^p, c^p \rangle, G' = \langle b^{p^2}, c^p \rangle$.

(3) $G = \langle a, b, c \mid a^{p^3} = b^{p^2} = c^p = 1, [b, c] = 1, [c, a] = b^p, [a, b] = a^{p^2} \rangle = (\langle a \rangle \rtimes \langle b \rangle) \rtimes \langle c \rangle$, 进一步地, $|G| = p^6$, $Z(G) = \Phi(G) = \langle a^p, b^p \rangle, G' = \langle a^{p^2}, b^p \rangle$.

证明 $\Longrightarrow$: 因为 $\mu(G) = p^3$ 且 $d(G) = 3$, 由引理 11.4.4 可知, $G' \cong \mathrm{C}_p^2$ 且 $c(G) = 2$. 这样的群是被安立坚等在文献 [8] 分类且 G 是 [8] 中的定理 4.7 中的群之一. 因为 $p > 2$, 故 G 是 [8] 中的定理 4.7 中的群 (A1)—(A3), (A7)—(A10), (B1)—(B3) 和 (C) 之一. 在这些群中找出满足定理条件的群即得定理中的群. 证明细节略去.

$\Longleftarrow$: 明显地, 定理中每个群含有一个 p^3 阶的非正规子群. 设 H 是 G 的阶 $\geqslant p^4$ 的子群. 下证 $H \unlhd G$.

若 $|G'\bigcap H|=1$, 则 $G=HZ(G)$. 于是 $H\trianglelefteq G$. 若 $|G'\bigcap H|=p^2$, 则 $G'\leqslant H$. 于是 $H\trianglelefteq G$. 若 $|Z(G)\bigcap H|\leqslant p$, 则 $G=HZ(G)$. 于是 $H\trianglelefteq G$. 若 $|Z(G)\bigcap H|\geqslant p^3$, 则 $G'\leqslant H$. 从而 $H\trianglelefteq G$.

上述论证表明, 我们可设 $|G'\bigcap H|=p$ 且 $|Z(G)\bigcap H|=p^2$. 令 $K\leqslant G'\bigcap H$ 且 $|K|=p$. 若 G 是群 (1a), 则 $G/K\cong \mathrm{M}_p(2,1,1)*\mathrm{C}_{p^3}$. 若 G 是群 (1b), 则 $G/K\cong \mathrm{M}_p(2,1,1)*\mathrm{C}_{p^2}$. 若 G 是群 (2), 则 $G/K\cong \mathrm{M}_p(2,1,1)*\mathrm{C}_{p^2}$. 若 G 是群 (3), 则 $G/K\cong \mathrm{M}_p(2,1,1)*\mathrm{C}_{p^2}$. 由定理 11.1.7 和定理 11.3.5 可知, $\mu(G/K)\leqslant p^2$. 特别地, $\mu(G/G'\bigcap H)\leqslant p^2$. 由此推出 $H/G'\bigcap H\trianglelefteq G/G'\bigcap H$. 因而 $H\trianglelefteq G$. □

定理 11.4.6 设 G 是有限 p 群, $\mu(G)=p^3$ 且 $|G'|=p^2$.

(1) 若 $d(G)=4$, 则 $|G|=p^6$;

(2) 若 $d(G)=5$, 则 $|G|=p^7$;

(3) 若 $d(G)\geqslant 4$, 则 $\mathrm{C}_p^2\cong G'=\Phi(G)\leqslant Z(G)$ 且 $\exp(G)\leqslant p^2$.

证明 由引理 11.4.4 可知, $G'\cong \mathrm{C}_p^2$ 且 $c(G)=2$. 由引理 11.1.2 可知, G 有一个 p 阶正规子群 N 满足 $N\leqslant G'$ 使得 G/N 不是 Dedekind 群. 因为 $\mu(G)=p^3$, 故 $\mu(G/N)\leqslant p^2$. 又 $|G'/N|=p$, 故 G/N 是定理 11.1.7 和定理 11.3.5 的群之一. 又 $N<G'$, 故 $d(G/N)=d(G)$.

若 $d(G)=d(G/N)=4$, 则 G/N 同构于下列群之一:

(A) $\mathrm{M}_p(1,1,1)*\mathrm{M}_p(1,1,1)$;

(B) $\mathrm{M}_p(1,1,1)*\mathrm{M}_p(m,1), (m\geqslant 2)$;

(C) $\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^n}\times \mathrm{C}_p, (n\geqslant 2)$.

若 G/N 同构于(A), 则 $|G|=p^6$. 若 G/N 同构于(B), 不妨设 $N=\langle x\rangle$ 且

$$G=\langle a,b,c,d,x\mid a^p=x^{i_1},b^p=x^{i_2},c^{p^m}=1,d^p=x^{i_4},x^p=1,[a,b]=c^{p^{m-1}}x^{i_5},\\ [c,d]=c^{p^{m-1}}x^{i_6},[a,c]=x^{i_7},[a,d]=x^{i_8},[b,c]=x^{i_9},[b,d]=x^{i_{10}}\rangle,$$

其中 $0\leqslant i_k\leqslant p-1, 1\leqslant k\leqslant 10$.

若 $|G|>p^6$, 则 $m\geqslant 3$. 我们将证明这种情况不可能发生.

情形 1 $i_1=i_2=0$.

若 $[a,c]\neq 1$ 且 $[b,c]\neq 1$, 则存在 $h\in G$ 使得 $[ab^h,c]=1$. 不妨设 $[a,c]=1$. 因为 $|\langle a,c\rangle|\geqslant p^4$, 故 $\langle a,c\rangle\trianglelefteq G$. 又 $x\notin\langle a,c\rangle$, 故 $[b,c]=[a,d]=1$, $[c,d]=[a,d]=c^{p^{m-1}}$. 类似地, 由 $[b,c]=1$ 推出 $[b,d]=1$. 于是 $G'=\langle c^{p^{m-1}}\rangle$. 这与 $|G'|=p^2$ 矛盾.

情形 2 i_1 和 i_2 至少有一个不为 0.

不妨设 $i_1\neq 0$. 若 $i_2\neq 0$, 对某个适当的 h, 用 ba^h 替换 b 则可得 $i_2=0$. 若 $i_4\neq 0$, 对某个适当的 h, 用 ad^h 替换 a 则可得 $i_1=0$. 这归结为情形 1.

设 $i_4=0$. 若 $i_9=0$, 因为 $|\langle b,c\rangle|\geqslant p^4$, 故 $\langle b,c\rangle\trianglelefteq G$. 因为 $x\notin\langle b,c\rangle$, 故 $[b,d]=[a,c]=1$, $[c,d]=[a,d]=c^{p^{m-1}}$. 类似地, 因为 $[b,d]=1$, 故 $[a,d]=1$. 于是

$G'=\langle c^{p^{m-1}}\rangle$. 这与 $|G'|=p^2$ 矛盾. 若 $i_9\neq 0$ 且 $i_{10}\neq 0$, 对某个适当的 h, 用 cd^h 替换 c 得 $[b,c]=1$. 这归结为 $i_9=0$ 的情形. 若 $i_9\neq 0$ 且 $i_{10}=0$, 则 $|\langle b,c^p,d\rangle|\geqslant p^4$ 且 $x\notin\langle b,c^p,d\rangle$. 另一方面, 因为 $[b,c]\in\langle b,c^p,d\rangle$, 故 $x\in\langle b,c^p,d\rangle$. 矛盾.

上述论证表明, 在任何情况下都导出矛盾. 故 $m=2$ 且 $|G|=p^6$.

若 G/N 同构于(C), 类似于上述论证仍有 $|G|=p^6$. 细节略去. 故 (1) 成立.

若 $d(G/N)=d(G)=5$, 则 $G/N\cong \mathrm{M}_p(1,1,1)*\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^n}$, $n\geqslant 2$. 令 $N=\langle x\rangle$ 且

$$\begin{aligned}G=\langle & a,b,c,d,e,x\mid a^p=x^{i_1},b^p=x^{i_2},c^p=x^{i_3},d^p=x^{i_4},e^{p^n}=x^{i_5},x^p=1,\\ &[a,b]=e^{p^{n-1}}x^{i_6},[c,d]=e^{p^{n-1}}x^{i_7},[a,c]=x^{i_8},[a,d]=x^{i_9},[a,e]=x^{i_{10}},\\ &[b,c]=x^{i_{11}},[b,d]=x^{i_{12}},[b,e]=x^{i_{13}},[c,e]=x^{i_{14}},[d,e]=x^{i_{15}}\rangle,\end{aligned}$$

其中 $0\leqslant i_k\leqslant p-1$, $1\leqslant k\leqslant 15$.

若 $|G|>p^7$, 则 $n\geqslant 3$. 因为 $c(G)=2$, 故 $G'=\langle e^{p^{n-1}},x\rangle$. 又 $G'\cong \mathrm{C}_p\times \mathrm{C}_p$, 故 $e^{p^n}=1$. 由 $[a,e]\in Z(G)$ 推出 $[e^p,a]=[e,a]^p=1$. 类似地, $[e^p,b]=[e^p,c]=[e^p,d]=1$. 于是 $e^p\in Z(G)$.

情形 1　$a^p=b^p=c^p=d^p=1$.

若 $[a,e],[b,e],[c,e]$ 和 $[d,e]$ 不为 1, 对某个适当的 h, 用 ab^h 替换 a 则可得 $[a,e]=1$. 设 $[a,e],[b,e],[c,e]$ 和 $[d,e]$ 至少有一个是 1. 不妨设 $[a,e]=1$. 因为 $|\langle a,e\rangle|>p^3$, 故 $\langle a,e\rangle\trianglelefteq G$. 又 $x\notin\langle a,e\rangle$, 故

$$[b,e]=[c,e]=[d,e]=[a,c]=[a,d]=1,\quad [a,b]=e^{p^{n-1}}.$$

因为 $[c,e]=1$, 故 $|\langle c,e\rangle|>p^3$. 因而 $\langle c,e\rangle\trianglelefteq G$. 又 $x\notin\langle c,e\rangle$, 故 $[b,c]=[b,d]=1$, $[c,d]=e^{p^{n-1}}$. 于是 $x\notin G'$, 矛盾.

情形 2　a^p,b^p,c^p 和 d^p 中至少有一个不是 1.

不妨设 $d^p=x\neq 1$. 分别用 ad^{h_1}, bd^{h_2} 和 cd^{h_3} 替换 a,b,c 可得 $a^p=b^p=c^p=1$. 若 $[a,e]\neq 1$ 且 $[b,e]\neq 1$, 用 ab^h 替换 a 可得 $[a,e]=1$. 不妨设 $[a,e]=1$. 因为 $|\langle a,e\rangle|>p^3$, 故 $\langle a,e\rangle\trianglelefteq G$. 又 $x\notin\langle a,e\rangle$, 故

$$[b,e]=[c,e]=[d,e]=[a,c]=[a,d]=1,\quad [a,b]=e^{p^{n-1}}.$$

因为 $[c,e]=1$, 故 $|\langle c,e\rangle|>p^3$. 因而 $\langle c,e\rangle\trianglelefteq G$. 因为 $x\notin\langle c,e\rangle$, 故 $[b,c]=[b,d]=1$, $[c,d]=e^{p^{n-1}}$. 于是 $x\notin G'$, 矛盾.

上述论证表明, 在任何情况下都导出矛盾. 故 $n=2$ 且 $|G|=p^7$. 故 (2) 成立.

由引理 11.4.4 可得, $G'\cong \mathrm{C}_p^2$ 且 $c(G)=2$. 由 (1) 和 (2) 可得 $|\Phi(G)|=p^2$. 因而 $\Phi(G)=G'\cong \mathrm{C}_p^2$. 对于任意元 $a\in G$, $a^p\in\Phi(G)$. 由此可得 $a^{p^2}=1$. 于是 $\exp(G)\leqslant p^2$, 即 (3) 成立. □

下述定理的证明篇幅较长, 在此仅列出结果, 证明过程略去, 有兴趣的读者可参看文献 [279] 的证明.

定理 11.4.7 设 G 是有限 p 群, $\mu(G)=p^3$. 则 $|G'|=p$ 当且仅当 G 是下列互不同构的群之一.

(1) $\mathrm{M}_p(1,1,1)*\mathrm{M}_p(1,1,1)*\mathrm{M}_p(m,1)$, $m\geqslant 2$, 此时 $|G|=p^{m+5}$, $Z(G)\cong \mathrm{C}_{p^{m-1}}$;

(2) $\mathrm{M}_p(1,1,1)*\mathrm{M}_p(1,1,1)*\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^n}$, $n\geqslant 1$, 此时 $|G|=p^{n+6}$, $Z(G)\cong \mathrm{C}_{p^n}$;

(3) $(\mathrm{M}_p(1,1,1)*\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^n})\times \mathrm{C}_p$, $n\geqslant 1$, 此时 $|G|=p^{n+5}$, $Z(G)\cong \mathrm{C}_{p^n}\times\mathrm{C}_p$;

(4) $(\mathrm{M}_p(1,1,1)*\mathrm{M}_p(m,1))\times \mathrm{C}_p$, $m\geqslant 2$, 此时 $|G|=p^{m+4}$, $Z(G)\cong \mathrm{C}_{p^{m-1}}\times \mathrm{C}_p$;

(5) $\mathrm{M}_p(1,1,1)*\mathrm{M}_p(2,1,1)*\mathrm{C}_{p^n}$, $n\geqslant 1$, 此时 $\mathrm{M}_p(1,1,1)\bigcap \mathrm{M}_p(2,1,1)=\mathrm{M}_p(2,1,1)\bigcap \mathrm{C}_{p^n}=\mathrm{M}_p'(2,1,1)$, $|G|=p^{n+5}$, $Z(G)\cong \mathrm{C}_{p^n}\times \mathrm{C}_p$;

(6) $\mathrm{M}_p(1,1,1)*\mathrm{M}_p(m,2)$, $m\geqslant 2$, 此时 $\mathrm{M}_p(1,1,1)\bigcap \mathrm{M}_p(m,2)=\mathrm{M}_p'(m,2)$, $|G|=p^{m+4}$, $Z(G)\cong \mathrm{C}_{p^{m-1}}\times \mathrm{C}_p$;

(7) $(\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^n})\times \mathrm{C}_{p^2}$, $n\geqslant 1$, 此时 $|G|=p^{n+4}$, $Z(G)\cong \mathrm{C}_{p^n}\times \mathrm{C}_{p^2}$;

(8) $(\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^n})\times \mathrm{C}_p^2$, $n\geqslant 1$, 此时 $|G|=p^{n+4}$, $Z(G)\cong \mathrm{C}_{p^n}\times \mathrm{C}_p\times \mathrm{C}_p$;

(9) $\mathrm{M}_p(m,1)\times \mathrm{C}_{p^2}$, $m\geqslant 2$, 此时 $|G|=p^{m+3}$, $Z(G)\cong \mathrm{C}_{p^{m-1}}\times \mathrm{C}_{p^2}$;

(10) $\mathrm{M}_p(3,1,1)*\mathrm{C}_{p^n}$, $n\geqslant 1$, 此时 $\mathrm{M}_p(3,1,1)\bigcap \mathrm{C}_{p^n}=\mathrm{M}_p'(3,1,1)$, $|G|=p^{n+4}$, $Z(G)\cong \mathrm{C}_{p^n}\times \mathrm{C}_{p^2}$;

(11) $\mathrm{M}_p(m,1)\times \mathrm{C}_p^2$, $m\geqslant 2$, 此时 $|G|=p^{m+3}$, $Z(G)\cong \mathrm{C}_{p^{m-1}}\times \mathrm{C}_p\times \mathrm{C}_p$;

(12) $\mathrm{M}_p(2,1,1)*\mathrm{M}_p(m,1)$, $m\geqslant 3$, 此时 $\mathrm{M}_p(2,1,1)\bigcap \mathrm{M}_p(m,1)=\mathrm{M}_p'(2,1,1)$, $|G|=p^{m+4}$, $Z(G)\cong \mathrm{C}_{p^{m-1}}\times \mathrm{C}_p$;

(13) $(\mathrm{M}_p(2,1,1)*\mathrm{C}_{p^n})\times \mathrm{C}_p$, $n\geqslant 1$, 此时 $\mathrm{M}_p(2,1,1)\bigcap \mathrm{C}_{p^n}=\mathrm{M}_p'(2,1,1)$, $|G|=p^{n+4}$, $Z(G)\cong \mathrm{C}_{p^n}\times \mathrm{C}_p\times \mathrm{C}_p$;

(14) $\mathrm{M}_p(m,2)\times \mathrm{C}_p$, $m\geqslant 2$, 此时 $|G|=p^{m+3}$, $Z(G)\cong \mathrm{C}_{p^{m-1}}\times \mathrm{C}_p\times \mathrm{C}_p$;

(15) $\mathrm{M}_p(2,2,1)*\mathrm{C}_{p^n}$, $n\geqslant 1$, 此时 $\mathrm{M}_p(2,1,1)\bigcap \mathrm{C}_{p^n}=\mathrm{M}_p'(2,1,1)$, $|G|=p^{n+4}$, $Z(G)\cong \mathrm{C}_{p^n}\times \mathrm{C}_p\times \mathrm{C}_p$;

(16) $\mathrm{M}_p(m,3)$, $m\geqslant 3$, 此时 $|G|=p^{m+3}$, $Z(G)\cong \mathrm{C}_{p^{m-1}}\times \mathrm{C}_{p^2}$.

最后介绍 $p=2$ 的情形.

[181] 中的定理 2.3 告诉我们: 对于有限 p 群 G 来说, 若 $\mu(G)=p^m>1$, 则 $|G'|\leqslant p^m$. 自然地, 我们依照 $|G'|$ 的可能情形分类 $\mu(G)=2^3$ 的有限 p 群 G. 鉴于篇幅所限, 这里只给出分类结果, 有兴趣的读者可参看文献 [278] 的证明.

定理 11.4.8 设 G 是有限 2 群, $\mu(G)=2^3$. 则

(Ⅰ) $|G'|=2^3$ 当且仅当 $G\cong\langle a,b,c\mid a^4=b^4=c^4=1,[a,b]=c^2,[a,c]=b^2c^2,[b,c]=a^2b^2,[c^2,a]=[c^2,b]=1\rangle$.

(Ⅱ) 若 $|G'|=2^2$ 且 $d(G)\geqslant 3$, 则 $|G|\leqslant 2^8$.

(Ⅲ) 若 $|G| \geqslant 2^9$, 则 $|G'| = 2^2$ 且 $d(G) = 2$ 当且仅当 $G \cong \langle a, b \mid a^{2^n} = b^4 = 1, [a, b] = a^{2^{n-2}} \rangle, n \geqslant 7$. 特别地, G 是亚循环的 $\mathcal{A}_2$ 群.

(IV) $|G'| = 2$ 当且仅当 G 是下列互不同构的群之一.

(1) $\mathrm{D}_8 * \mathrm{D}_8 * \mathrm{M}_2(m, 1), m \geqslant 3$;

(2) $\mathrm{D}_8 * \mathrm{D}_8 * \mathrm{D}_8 * \mathrm{C}_{2^n}, n \geqslant 1$;

(3) $\mathrm{D}_8 * \mathrm{D}_8 * \mathrm{D}_8 * \mathrm{Q}_8$;

(4) $(\mathrm{D}_8 * \mathrm{D}_8 * \mathrm{Q}_8) \times \mathrm{C}_2$;

(5) $(\mathrm{D}_8 * \mathrm{D}_8 * \mathrm{C}_{2^n}) \times \mathrm{C}_2, n \geqslant 1$;

(6) $(\mathrm{D}_8 * \mathrm{M}_2(m, 1)) \times \mathrm{C}_2, m \geqslant 3$;

(7) $\mathrm{D}_8 * \mathrm{M}_2(2, 1, 1) * \mathrm{C}_{2^n}$, 其中 $\mathrm{D}_8 \bigcap \mathrm{M}_2(2, 1, 1) = \mathrm{M}_2(2, 1, 1) \bigcap \mathrm{C}_{2^n} = \mathrm{M}_2'(2, 1, 1)$;

(8) $\mathrm{D}_8 * \mathrm{Q}_8 * \mathrm{M}_2(2, 1, 1)$, 其中 $\mathrm{Q}_8 \bigcap \mathrm{M}_2(2, 1, 1) = \mathrm{M}_2'(2, 1, 1)$;

(9) $(\mathrm{D}_8 * \mathrm{Q}_8) \times \mathrm{C}_4$;

(10) $\mathrm{D}_8 * \mathrm{M}_2(m, 2)$, 其中 $m \geqslant 3, \mathrm{D}_8 \bigcap \mathrm{M}_2(m, 2) = \mathrm{M}_2'(m, 2)$;

(11) $(\mathrm{D}_8 * \mathrm{Q}_8) \times \mathrm{C}_2^2$;

(12) $(\mathrm{D}_8 * \mathrm{C}_{2^n}) \times \mathrm{C}_{2^2}, n \geqslant 1$;

(13) $(\mathrm{D}_8 * \mathrm{C}_{2^n}) \times \mathrm{C}_2^2, n \geqslant 3$;

(14) $\mathrm{M}_2(m, 1) \times \mathrm{C}_{2^2}, m \geqslant 3$;

(15) $\mathrm{M}_2(3, 1, 1) * \mathrm{C}_{2^n}$, 其中 $n \geqslant 1, \mathrm{M}_2(3, 1, 1) \bigcap \mathrm{C}_{p^n} = \mathrm{M}_2'(3, 1, 1)$;

(16) $\mathrm{M}_2(m, 1) \times \mathrm{C}_2^2, m \geqslant 3$;

(17) $\mathrm{M}_2(2, 1, 1) * \mathrm{M}_2(m, 1)$, 其中 $m \geqslant 3$, $\mathrm{M}_2(2, 1, 1) \bigcap \mathrm{M}_2(m, 1) = \mathrm{M}_2'(2, 1, 1)$;

(18) $(\mathrm{M}_2(2, 1, 1) * \mathrm{C}_{2^n}) \times \mathrm{C}_2$, 其中 $n \geqslant 1$, $\mathrm{M}_2(2, 1, 1) \bigcap \mathrm{C}_{p^n} = \mathrm{M}_2'(2, 1, 1)$;

(19) $(\mathrm{M}_2(2, 1, 1) * \mathrm{Q}_8) \times \mathrm{C}_2$, 其中 $\mathrm{M}_2(2, 1, 1) \bigcap \mathrm{Q}_8 = \mathrm{M}_2'(2, 1, 1)$;

(20) $\mathrm{M}_2(3, 1, 1) * \mathrm{Q}_8$, 其中 $\mathrm{M}_2(2, 1, 1) \bigcap \mathrm{Q}_8 = \mathrm{M}_2'(3, 1, 1)$;

(21) $\mathrm{Q}_8 \times \mathrm{C}_{2^3}$;

(22) $\mathrm{Q}_8 \times \mathrm{C}_{2^2} \times \mathrm{C}_2$;

(23) $\mathrm{M}_2(m, 2) \times \mathrm{C}_2, m \geqslant 1$;

(24) $\mathrm{M}_2(2, 2, 1) * \mathrm{C}_{2^n}$, 其中 $n \geqslant 1, \mathrm{M}_2(2, 1, 1) \bigcap \mathrm{C}_{p^n} = \mathrm{M}_2'(2, 1, 1)$;

(25) $\mathrm{M}_2(m, 3), m \geqslant 3$.

11.5 非正规子群的正规闭包均同阶的 p 群

就像我们前面看到的, 张勤海等[278, 279] 从非正规子群阶的角度部分推广了 Passman[181] 的结果. 王丽芳等[228] 则从非正规子群的正规闭包的角度也部分推广了 Passman[181] 的结果. 该文研究了非正规子群的正规闭包均同阶的有限群, 特别

是分类了非正规子群的正规闭包均同阶的有限 p 群. 王丽芳在文献 [230] 也分类了非正规内交换子群的正规闭包是极大子群的亚循环 p 群. 本节内容取自 [228].

令 $\Delta(G) = \{|H^G| \mid H \ntrianglelefteq G\}$, 其中 $H \leqslant G$, G 是有限群. 以 $\Delta(G)$ 的术语, G 的非正规子群的正规闭包均同阶等价于 $|\Delta(G)| = 1$. $\Delta(G)$ 的大小可看作是 G 离 Dedekind 群 "多远" 的一个度量, 显然, G 是 Dedekind 群当且仅当 $\Delta(G) = \varnothing$. Passman 在文献 [181] 分类的阶 $\geqslant p^2$ 的子群均正规的 p 群恰是 $|\Delta(G)| = 1$ 且 $\Delta(G) = \{p^2\}$ 的 p 群. 张勤海等在文献 [275] 分类的阶 $\geqslant p^3$ 的子群均正规的 p 群恰是 $\Delta(G) = \{p^2, p^3\}$ 的 p 群. 张勤海等在文献 [278], [279] 分类的阶 $\geqslant p^4$ 的子群均正规的 p 群恰是 $\Delta(G) = \{p^2, p^3, p^4\}$ 的 p 群.

为方便, $|\Delta(G)| = 1$ 的有限群 G 简记为 Δ_1 群. 本节介绍 Δ_1 群的结果.

由 Δ_1 群的定义可得如下结论.

引理 11.5.1 设 G 是 Δ_1 群. 若 $N \trianglelefteq G$ 且 G/N 不是 Dedekind 群, 则 G/N 是 Δ_1 群.

引理 11.5.2 设 G 是 Δ_1 群. 若 M 为 G 的非正规极大子群, 则

(1) 若 $H \ntrianglelefteq G$, 则 $H^G = G$;

(2) 若 L 是 G 的非平凡正规子群, 则 L 的每个子群在 G 中正规. 特别地, G 是 T 群. (G 称 T 群, 若 $H \trianglelefteq K \trianglelefteq G$, 则 $H \trianglelefteq G$.)

定理 11.5.3 设 G 是有限可解非幂零群. 则 G 是 Δ_1 群当且仅当 $G = L \rtimes \langle x \rangle$, 其中 L 为 G 的正规交换 p'-Hall 子群, $\langle x \rangle$ 为 G 的 p-Sylow 子群, x 在 L 上诱导出 p 阶无不动点自同构, p 为 $|G|$ 的最小素因子.

证明 $\Longrightarrow$: 设 G 是 Δ_1 群, 由于 G 可解非幂零, 故 G 中存在非正规极大子群 M 以及正规极大子群 K. 设 H 为 G 的非正规子群, 由引理 11.5.2 可知, $H^G = G$ 且 K 的每个子群在 G 中正规. 故 G 有一个主群列使得每个主因子为循环的. 因而 G 超可解.

设 p 是 $|G|$ 的最小素因子, G_p 为 G 的 p-Sylow 子群, L 为 G 的 p'-Hall 子群, 由于 G 有 Sylow 塔性质, 故 $L \trianglelefteq G$. 由引理 11.5.2 (2) 可知, L 的子群均在 G 中正规. 因此 $G_q \trianglelefteq G$, 其中 $G_q \in \mathrm{Syl}_q(G)$ 且 $q \neq p$. 由于 G 非幂零, 故 G_p 在 G 中非正规. 若 G_p 非循环, 则 G_p 中存在两个极大子群 P_1 和 P_2 使得 $G_p = P_1P_2$. 由于 $|G : LP_i| = p$ 且 p 是 $|G|$ 的最小素因子, 故 $LP_i \trianglelefteq G$. 由引理 11.5.2 可知, $P_i \trianglelefteq G$, $i = 1, 2$. 因而 $G_p = P_1P_2 \trianglelefteq G$, 矛盾. 故 G_p 循环.

设 $G_p = \langle x \rangle$, 则 $G = L \rtimes \langle x \rangle$. 由于 $L\langle x^p \rangle \trianglelefteq G$, 由引理 11.5.2 可知, L 的每个子群在 G 中正规且 $\langle x^p \rangle \trianglelefteq G$. 因而 x 依共轭作用在 L 上诱导出 p 阶幂自同构. 由于 p 为 $|G|$ 的最小素因子且 L 为 G 的 p'-Hall 子群, 故 L 为奇阶 Dedekind 群. 因而 L 交换.

下证 $C_L(x) = 1$. 若否, 由 [116] 中的 8.4.2 可知, $L = [L, x] \times C_L(x)$. 由于 $G = L\langle x\rangle$, 故 $\langle x\rangle^G \leqslant [L, x]\langle x\rangle \neq G$, 矛盾. 故 $C_L(x) = 1$.

$\Longleftarrow$: 由于 $C_L(x) = 1$, 故 $[L, \langle x\rangle] = L$. 显然 $[L, \langle x\rangle] \leqslant \langle x\rangle^G$. 因而, $L\langle x\rangle \leqslant \langle x\rangle^G$. 进而 $\langle x\rangle^G = G$. 又 $[L, x^p] = 1$ 且 $\langle x^p\rangle$ 为 $\langle x\rangle$ 的极大子群, 故 $O_p(G) = \langle x^p\rangle$.

设 H 为 G 的任意非正规子群, $H_p \in \mathrm{Syl}_p(H)$. 若 $p \mid |G : H|$, 则 $H_p \leqslant O_p(G)$ 且 $H_p \trianglelefteq G$. 由于 $H \bigcap L \trianglelefteq G$ 且 $H = (H \bigcap L)H_p$, 故 $H \trianglelefteq G$, 矛盾. 因而 $p \nmid |G : H|$, 进而 H 包含 G 的一个 p-Sylow 子群. 不妨设 $\langle x\rangle \leqslant H$, 则 $H^G \geqslant \langle x\rangle^G = G$. 因而 $H^G = G$. 故 G 是 Δ_1 群. □

引理 11.5.4 *设 G 是有限非可解 Δ_1 群, K/L 是 G 的非可解主因子, 则 $K = G$ 且 G/L 是非交换单群.*

证明　设 $K/L \cong T^n$, 其中 T 是非交换单群, T_1 是 T 的非正规子群, 则 $T_1^n \ntrianglelefteq T^n$. 由 $K/L \cong T^n$ 可知, 存在 K/L 的子群 H/L 使得 $H/L \cong T_1^n$, $H/L \ntrianglelefteq K/L$ 且 $(H/L)^{K/L} = K/L$, 进而 $H^K = K$. 由 $K \trianglelefteq G$ 可得, $H^G \leqslant K$. 由此可得, $H^G = K$.

由于 G 非可解, 故 G 有非正规极大子群. 由引理 11.5.2 可得, $K = G$. 因而 $n = 1$ 且 G/L 是非交换单群. □

引理 11.5.4 告诉我们, 对于非可解的 Δ_1 群 G 来讲, G 的每个主群列中第一个主因子是该群列中唯一的不可解的主因子. 由引理 11.5.4 还可得下面的推论.

推论 11.5.5 *设 G 是有限非可解 Δ_1 群.*

(1) *若 M 是 G 的极大正规子群, 则 G/M 是非交换单群;*

(2) *若 N 是 G 的真正规子群, 则 G/N 非可解.*

推论 11.5.5 的一个直接结果是非可解的 Δ_1 群是完全群.

定理 11.5.6 *设 G 是有限非可解群. 则 G 是 Δ_1 群当且仅当 $G/Z(G)$ 是非交换单群且 $Z(G) = \Phi(G)$.*

证明　$\Longleftarrow$: 由引理 11.5.2, 我们只需证明: 对 G 的非正规子群 H, 有 $H^G = G$.

由 $H \ntrianglelefteq G$ 及 $Z(G) = \Phi(G)$ 可得, $Z(G) < HZ(G) < G$. 由于 $G/Z(G)$ 为非交换单群, 故 $HZ(G)/Z(G) \ntrianglelefteq G/Z(G)$ 且 $(HZ(G)/Z(G))^{G/Z(G)} = G/Z(G)$. 因而 $(HZ(G))^G = H^G Z(G) = G$. 由 $Z(G) = \Phi(G)$ 可知, $H^G = G$.

$\Longrightarrow$: 设 N 是 G 的极大正规子群. 由推论 11.5.5 和引理 11.5.2 可得, G/N 为非交换单群且 N 的每个子群在 G 中正规. 因而 $G/C_G(N) \lesssim \mathrm{Pot}(N)$, 其中 $\mathrm{Pot}(N)$ 为 N 的幂自同构群. 由于 $\mathrm{Pot}(N)$ 交换, 故 $G/C_G(N)$ 交换. 注意到 G 是完全群, 故 $G' = G$, 因此 $C_G(N) = G$. 进而有 $N \leqslant Z(G)$. 由于 N 为 G 的极大正规子群, 故 $N = Z(G)$.

任取 G 的极大子群 L. 若 $Z(G) \nleqslant L$, 则 $G = LZ(G)$ 且 $L \trianglelefteq G$. 进而有 G/L 交换, 矛盾于 11.5.5(1). 因而 $Z(G) \leqslant L$. 由 L 的任意性可得, $Z(G) \leqslant \Phi(G)$. 由于 $G/Z(G)$ 为单群, 故 $Z(G) = \Phi(G)$. □

注 11.5.7 非可解非单的 Δ_1 群存在. 例如, 设 $G=\mathrm{SL}_2(5)$. 则 $Z(G)=\Phi(G)$ 且 $G/Z(G)\cong \mathrm{A}_5$. 由定理 11.5.6 可知, G 是非可解的 Δ_1 群.

下面讨论幂零的 Δ_1 群. 我们将证明幂零的 Δ_1 群为 p 群. 然后分类 Δ_1-p 群.

定理 11.5.8 若 G 是有限幂零的 Δ_1 群, 则 G 为 p 群.

证明 由于 G 为 Δ_1 群, 故 G 不是 Dedekind 群. 因而存在 G 的 p-Sylow 子群 P 使得 P 不为 Dedekind 群. 令 $G=P\times H$, 其中 H 是 G 的 p'-Hall 子群.

若 $H\neq 1$, 取 P 的非正规子群 K, 则 $K\ntrianglelefteq G$ 且 $K\times H\ntrianglelefteq G$. 由 $K^G=K^P$ 及 $(K\times H)^G=K^P\times H$ 可得, $|K^G|\neq|(K\times H)^G|$, 矛盾. 因而 $H=1$, 即 G 为 p 群. □

引理 11.5.9 设 G 是有限 p 群, $|G'|=p$. 则 G 是 Δ_1 群当且仅当 G 的非正规子群同阶. 进一步地, G 是 [28] 中的定理 112.3、定理 112.4 列出的群之一.

证明 设 H 为 G 的非正规子群, 由于 $|G'|=p$, 故 $H^G=HG'$ 且 $|H^G:H|=p$. 由题设可知, 结论成立. □

下面分 $p>2$ 和 $p=2$ 两种情形给出 Δ_1-p 群的结构.

引理 11.5.10 设 p 为奇素数, Z_p 为模 p 的整数集. 若 u,w 为整数且 $u+\dfrac{w^2}{4}\not\equiv 0 \pmod p$, 其中 $\dfrac{1}{4}$ 为 4 在 Z_p 中的逆, 则存在 i,j 使得 $i^2-uj^2+wij-ni+mj+l\equiv 0 \pmod p$.

证明 计算可得

$$\begin{aligned}
i^2-uj^2+wij-ni+mj+l=&\left(i-\frac{n}{2}+\frac{w}{2}j\right)^2-\left(u+\frac{w^2}{4}\right)\\
&\times\left(j-\frac{m+\frac{n}{2}w}{2}\left(u+\frac{w^2}{4}\right)^{-1}\right)^2\\
&+\frac{\left(m+\frac{n}{2}w\right)^2}{4}\left(u+\frac{w^2}{4}\right)^{-1}+l-\frac{n^2}{4}\\
\equiv&\, 0 \pmod p,
\end{aligned}$$

其中 $\left(u+\dfrac{w^2}{4}\right)^{-1}$ 为 $u+\dfrac{w^2}{4}$ 在 Z_p 中的逆.

令

$$\begin{aligned}
&i'\equiv i-\frac{n}{2}+\frac{w}{2}j \pmod p,\\
&u'\equiv u+\frac{w^2}{4} \pmod p,\\
&j'\equiv j-\frac{m+\frac{n}{2}w}{2}\left(u+\frac{w^2}{4}\right)^{-1} \pmod p,\\
&v'\equiv \frac{\left(m+\frac{n}{2}w\right)^2}{4}\left(u+\frac{w^2}{4}\right)^{-1}+l-\frac{n^2}{4} \pmod p.
\end{aligned}$$

则 $i'^2 \equiv u'j'^2 - v' \pmod p$.

设 $A = \{i'^2 \mid i' \in Z_p\}$ 且 $B = \{u'j'^2 - v' \mid j' \in Z_p\}$. 由于 $|A| = |B| = \dfrac{p-1}{2} + 1$, 故 $A \bigcap B \neq \varnothing$. 因而存在 i, j 使得 $i^2 - uj^2 + wij - ni + mj + l \equiv 0 \pmod p$. □

定理 11.5.11 设 G 是有限 p 群, $p > 2$. 则 G 是 Δ_1 群当且仅当 G 同构于下列互不同构的群之一.

(1) $\mathrm{M}_p(n, m), n \geqslant m$;

(2) $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n}$;

(3) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [a,b] = 1, [a,c] = b^p, [b,c] = a^p b^{wp}\rangle$, 其中 $1 \leqslant w \leqslant \dfrac{p-1}{2}$ 且 $1 + \dfrac{w^2}{4}$ 为模 p 的平方非剩余;

(4) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [a,b] = 1, [a,c] = b^{vp}, [b,c] = a^p b^{wp}\rangle$, 其中 v 是模 p 平方非剩余, $0 \leqslant w \leqslant \dfrac{p-1}{2}$ 且 $v + \dfrac{w^2}{4}$ 是模 p 的平方非剩余.

证明 设 G 是 Δ_1 群. 对 $|G|$ 作归纳.

若 $|G'| = p$, 由引理 11.5.9 可得群 (1) 和 (2). 下面假设 $|G'| \geqslant p^2$.

取 $N \trianglelefteq G$ 满足: $N \leqslant G'$ 且 $|N| = p$. 显然 $N \leqslant Z(G)$. 令 $\overline{G} = G/N$. 由引理 11.13.3 可知, $\overline{G}$ 为 Δ_1 群. 因而, $\overline{G}$ 同构于定理中的群. 分三种情形讨论.

情形 1 $\overline{G} \cong \mathrm{M}_p(n, m)$.

由定理 6.1.2 可知, $G = \langle a, b \mid a^{p^{n+1}} = b^{p^m} = 1, [a,b] = a^{p^{n-1}}\rangle, n \geqslant 2, m \geqslant 2$. 取 $H = \langle b\rangle, K = \langle b^p\rangle$. 显然, $H \ntrianglelefteq G$, $K \ntrianglelefteq G$. 然而, $|H^G| \neq |K^G|$. 因而这种情形不可能发生.

情形 2 $\overline{G} \cong \mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n}$.

由于 $|\overline{G}'| = |(G/N)'| = p$ 且 $N \leqslant G'$, 故 $|G'| = p^2$. 由引理 11.3.6 和定理 11.3.7 可得, G 为群 (3) 或 (4).

情形 3 $\overline{G} \cong \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^2} = \bar{b}^{p^2} = \bar{c}^p = 1, [\bar{a}, \bar{b}] = 1, [\bar{a}, \bar{c}] = \bar{b}^{up}, [\bar{b}, \bar{c}] = \bar{a}^p \bar{b}^{wp}\rangle$, 其中 $u = 1$ 或 v, v 是模 p 的平方非剩余且 $u + \dfrac{w^2}{4}$ 为模 p 的平方非剩余.

令 $N = \langle x\rangle$, 则可设

$$G = \langle a, b, c \mid a^{p^2} = x^i, b^{p^2} = x^j, c^p = x^k, [a,b] = x^l, [a,c] = b^{up} x^m,$$
$$[b,c] = a^p b^{wp} x^n, x^p = 1, [x,a] = [x,b] = [x,c] = 1\rangle,$$

其中 i, j, k, l, m, n 为整数且其中至少有一个与 p 互素.

由 $G_3 \leqslant N$ 可知, $|G_3| \leqslant p$. 因而 G 亚交换. 由命题 1.1.9 可得

$$1 = [a, c^p] = [a,c]^p [a,c,c]^{\binom{p}{2}} = [a,c]^p = b^{up^2}.$$

因而, $b^{p^2}=1$.

由于 $c^p\in Z(G)$ 且 $\exp(G_3)\leqslant p$, 故

$$1=[b,c^p]=[b,c]^p[b,c,c]^{\binom{p}{2}}=[b,c]^p=a^{p^2}.$$

因此 $a^{p^2}=1$. 由

$$[a^p,b]=[a,b]^p[a,b,a]^{\binom{p}{2}}=[a,b]^p=1$$

和

$$[a^p,c]=[a,c]^p[a,c,a]^{\binom{p}{2}}=[b^{up},a]^{\binom{p}{2}}=1$$

可得, $a^p\in Z(G)$. 同理可得, $b^p\in Z(G)$. 因而, $G'\leqslant Z(G)$ 且 $G'\cong C_p^3$.

假设 $c^p=1$. 显然, $\langle a\rangle\ntrianglelefteq G$ 且 $\langle c\rangle\ntrianglelefteq G$. 由于 $G'\leqslant Z(G)$, 故

$$\langle a\rangle^G=\langle a,[a,b],[a,c]\rangle,\quad \langle c\rangle^G=\langle c,[a,c],[b,c]\rangle.$$

从而 $|\langle a\rangle^G|=p^4$ 且 $|\langle c\rangle^G|=p^3$, 矛盾. 因而, $c^p\neq 1$.

此时, 可设

$$\begin{aligned}G=&\langle a,b,c\mid a^{p^2}=b^{p^2}=c^{p^2}=1,[a,b]=c^{lp},[a,c]=b^{up}c^{mp},\\&[b,c]=a^pb^{wp}c^{np},[c^p,a]=[c^p,b]=1\rangle.\end{aligned}$$

显然 $c(G)=2$ 且 $\exp(G')=p$.

下证: 存在 G 的子群 H 同构于 $M_p(2,2)$ 或 $C_{p^2}\times C_{p^2}$.

设 $x=ac^i,y=bc^j$, 则

$$\begin{aligned}[x,y]&=[ac^i,bc^j]\\&=a^{-ip}b^{(ju-iw)p}c^{(l+jm-in)p}\\&=(ac^i)^{-ip}(bc^j)^{(ju-iw)p}c^{(i^2-uj^2+wij-ni+mj+l)p}\\&=x^{-ip}y^{(ju-iw)p}c^{(i^2-uj^2+wij-ni+mj+l)p}.\end{aligned}$$

由引理 11.5.10 可知, 存在 i',j' 使得 $i'^2-uj'^2+wi'j'-ni'+mj'+l\equiv 0\pmod p$.

令 $x'=ac^{i'},y'=bc^{j'}$ 且 $H=\langle x',y'|x'^{p^2}=y'^{p^2}=1,[x',y']=x'^{-i'p}y'^{(j'u-i'w)p}\rangle$. 易见, $H\cong M_p(2,2)$ 或 $C_{p^2}\times C_{p^2}$.

若 $H\trianglelefteq G$, 由于 $|G/H|=p^2$, 故 G/H 交换. 因而, $G'\leqslant\Omega_1(G)\bigcap H=\Omega_1(H)$. 另一方面, $\Omega_1(H)\cong C_p^2$, 矛盾. 因而, $H\ntrianglelefteq G$ 且 $|H^G|>p^4$.

由于 $|\langle a\rangle^G|=p^4$, $|H^G|\neq|\langle a\rangle^G|$, 矛盾. 因此, 这种情形不可能发生.

反过来, 我们证明定理中所列的群为互不同构的 Δ_1 群. 容易证明定理中所列的群互不同构. 下证它们是 Δ_1 群.

由 [28] 中的定理 112.3、定理 12.4 和引理 11.5.9 可知, 群 (1) 和 (2) 为 Δ_1 群. 设 G 是群 (3) 或 (4), 显然 $|G'|=p^2$ 且 $Z(G)=G'=\langle a^p,b^p\rangle$. 设 H 为 G 的任意非正规子群.

若 $H\bigcap G'\neq 1$, 则 $|H\bigcap G'|=p$. 令 $N=H\bigcap G'$, 则 $\overline{G}=G/N\cong \mathrm{M}_p(1,1,1)*\mathrm{C}_{p^n}$ 且 $\overline{H}\ntrianglelefteq\overline{G}$. 由定理 11.1.7 可知, $\overline{G}$ 的非正规子群均为 p 阶. 因此 $|\overline{H}^{\overline{G}}|=|\overline{H^G}|=p^2$. 所以, $|H^G|=p^3$.

若 $H\bigcap G'=1$, 则 $H\bigcap \mho_1(G)=1$ 且 H 交换. 若 $\exp(H)=p^2$, 则 $H\bigcap\mho_1(G)\neq 1$, 矛盾. 因而, $\exp(H)=p$ 且 $H\leqslant\Omega_1(G)=\langle a^p,b^p,c\rangle$. 进而有 $H=\langle h\rangle$, 其中 $h=a^{ip}b^{jp}c$. 显然 $[a,h]=[a,c],[b,h]=[b,c]$. 因此 $G'\leqslant\langle h\rangle^G$ 且 $\langle h\rangle^G=\langle h\rangle G'=H^G$. 所以, $|H^G|=p^3$. □

定理 11.5.12　设 G 为有限 2 群. 则 G 是 Δ_1 群当且仅当 G 同构于下列互不同构的群之一.

(1) $\mathrm{M}_2(n,m), n\geqslant m$;

(2) $G=\langle a,b,c\mid a^{2^n}=b^2=c^2=1,[b,c]=a^{2^{n-1}},[a,b]=[a,c]=1\rangle\cong \mathrm{D}_8*\mathrm{C}_{2^n}$;

(3) $G=\langle a,b,c,d\mid a^4=b^2=1,[a,b]=a^2,c^2=d^2=a^2,[c,d]=a^2,[a,c]=[a,d]=[b,c]=[b,d]=1\rangle\cong \mathrm{Q}_8*\mathrm{D}_8$;

(4) $G=\langle a,b,c\mid a^4=1,b^2=a^2,[a,b]=a^2,c^4=1,[c,a]=[c,b]=1\rangle\cong \mathrm{Q}_8\times \mathrm{C}_4$;

(5) G 为 2^n 阶极大类 2 群;

(6) $G=\langle a,b\mid a^{2^n}=b^4=1,[a,b]=a^{-2}\rangle, n\geqslant 3$;

(7) $G=\langle a,b\mid a^{2^n}=b^4=1,[a,b]=a^{-2+2^{n-1}}\rangle, n\geqslant 3$;

(8) $G=\langle a,b,c\mid a^4=b^4=c^2=1,[a,b]=1,[a,c]=b^2,[b,c]=a^2b^2\rangle$;

(9) $G=\langle a,b,c\mid a^4=b^4=1,c^2=b^2,[a,b]=1,[a,c]=b^2,[b,c]=a^2\rangle$;

(10) $G=\langle a,b,c,d\mid a^4=b^4=1,c^2=a^2b^2,d^2=a^2,[a,b]=a^2,[c,d]=a^2b^2,[a,c]=[b,d]=1,[b,c]=[a,d]=b^2\rangle$;

(11) $G=\langle a,b,c\mid a^4=b^4=c^4=1,[a,b]=c^2,[c,a]=b^2c^2,[c,b]=a^2b^2,[c^2,a]=[c^2,b]=1\rangle$.

证明　设 G 是 Δ_1 群, 对 $|G|$ 作归纳.

若 $|G'|=p$, 由 [28] 中的定理 112.3、定理 112.4 和引理 11.5.9 可得群 (1)—(4). 下设 $|G'|\geqslant p^2$.

由引理 11.1.2 可知, 存在 G' 的极大子群 K 使得 $K\trianglelefteq G$ 且 G/K 不是 Dedekind 群. 设 N 为含于 K 的 G 的 p 阶正规子群, 则 $N\leqslant Z(G)$. 令 $\overline{G}=G/N$. 由引理 11.5.1 可知, $\overline{G}$ 为 Δ_1 群. 因而, $\overline{G}$ 同构于定理中所列的群之一. 类似于定理 11.5.11, 对 $\overline{G}$ 分情况作扩张即得定理中的群. 细节略去.

反过来, 我们证明定理中所列的群互不同构且均为 Δ_1 群.

通过比较导群的阶、生成元个数、幂零类等 G 的型不变量可知, 定理中所列的群互不同构. 下证群 (1)—(11) 均为 Δ_1 群.

由 [28] 中的定理 112.3、定理 112.4 和引理 11.5.9 可知, 群 (1)—(4) 为 Δ_1 群.

若 G 为群 (5), (6) 或 (7), 则 G 有交换极大子群 A 使得 A 的每个子群在 G 中正规. 设 H 为 G 的任一非正规子群, 则存在 $h \in H \backslash A$. 断言 $\langle h\rangle^G$ 为 G 的极大子群: 设 $h = bx$, 其中 $x \in A$. 由于 $\langle [a,h]\rangle = \langle [a,b]\rangle = \langle a^2\rangle \leqslant \langle h\rangle^G$, $h^2 = (bx)^2 = b^2$ 或 $b^2a^{2^{n-1}}$, 故 $b^2 \in \langle h\rangle^G$. 进而有 $\Phi(G) \leqslant \langle h\rangle^G$. 由 $h \notin \Phi(G)$ 可得, $\langle h\rangle^G = \langle h\rangle\Phi(G)$ 为 G 的极大子群. 因此 $H^G = \langle h\rangle^G$. 故 G 是 Δ_1 群.

设 G 为群 (8), H 为 G 的任一非正规子群. 显然 $Z(G) = G' = \langle a^2, b^2\rangle$. 考虑 $H \bigcap G'$. 下证 $|H^G| = 8$.

若 $H \bigcap G' \neq 1$, 则 $|H \bigcap G'| = 2$. 令 $N = H \bigcap G'$, 则 $\overline{G} = G/N \cong \mathrm{D}_8 * \mathrm{C}_4$ 且 $\overline{H} \ntrianglelefteq \overline{G}$. 由定理 11.1.7 可知, $\overline{G}$ 是 Δ_1 群且 $|\overline{H}^{\overline{G}}| = |\overline{H^G}| = 4$. 因此, $|H^G| = 8$.

若 $H \bigcap G' = 1$, 则 $H \bigcap \mho_1(G) = 1$. 若 $\exp(H) = 4$, 则 $H \bigcap \mho_1(G) \neq 1$, 矛盾. 因此, $\exp(H) = 2$, $H \leqslant \Omega_1(G) = \langle a^2, b^2, c\rangle$ 且 $H^G \leqslant \Omega_1(G)$. 由于 $H \bigcap G' = 1$, 故存在 $h \in H$ 使得 $h = a^{2i}b^{2j}c$. 显然 $[a,h] = [a,c], [b,h] = [b,c]$. 因此 $G' \leqslant \langle h\rangle^G$ 且 $\langle h\rangle^G = \langle h\rangle G' = \Omega_1(G) \leqslant H^G$. 因而 $\Omega_1(G) = H^G$. 从而 $|H^G| = 8$.

设 G 为群 (9) 或 (10), H 为 G 的任一非正规子群. 显然, $Z(G) = G' = \Omega_1(G) = \langle a^2, b^2\rangle$. 由定理 11.2.1 可知, H 为 4 阶循环群. 因而 $H^G = HG'$ 且 $|H^G| = 8$.

设 G 为群 (11), 则 $Z(G) = G' = \Omega_1(G) = \langle a^2, b^2, c^2\rangle$. 由 [246] 中的定理 5.2 可知, G 为无交换极大子群的 $\mathcal{A}_2$ 群. 因此 G 的每个极大子群 M 均内交换且 $\Phi(G) = \Phi(M)$ 含于 G 的任一二极大子群. 因而 G 的每个二极大子群正规. 设 H 为 G 的任一非正规子群, 则 $|H| \leqslant 2^3$ 且 $\exp(H) = 4$. 因此, H 交换且 $H \cong \mathrm{C}_4$ 或 $\mathrm{C}_4 \times \mathrm{C}_2$. 任取 H 的 4 阶元 h, 则 $H = \langle h\rangle(H \bigcap G')$ 且 $H^G = \langle h\rangle^G(H \bigcap G')$. 计算可知, $\langle h\rangle^G = \langle h\rangle G'$. 因而, $H^G = \langle h\rangle G'$ 且 $|H^G| = 2^4$. □

设 G 为 p^n 阶非 Dedekind 群, 若 H 为 G 的非正规子群, 则 $p^2 \leqslant |H^G| \leqslant p^{n-1}$, 即 $1 \leqslant |\Delta(G)| \leqslant n-2$. 一个自然的问题是: *任意给定 $k \in \{1, 2, \cdots, n-2\}$, 是否存在 p^n 阶群 G 使得 $|\Delta(G)| = k$?* 下面的例子告诉我们答案是肯定的. 也就是说, $|\Delta(G)|$ 可以为任意正整数.

例 11.5.13 设 $G \cong \mathrm{M}_p(n-k, 1) \times \mathrm{C}_p^{k-1}$. 则 $|\Delta(G)| = k$.

证明 不妨设 $G = \langle a, b, c_1, \cdots, c_{k-1} \mid a^{p^{n-k}} = b^p = 1, [a,b] = a^{p^{n-k-1}}, [a, c_i] = [b, c_i] = [c_i, c_j] = 1\rangle$. 则 G 为 p^n 阶群. 若 H 为 G 的阶 $\geqslant p^{k+1}$ 的子群, 则 $H \bigcap \langle a\rangle \neq 1$. 由于 $G' = \langle a^{p^{n-k-1}}\rangle \leqslant H$, 故 $H \trianglelefteq G$. 因而 G 的非正规子群的阶 $\leqslant p^k$.

令 $H_0 = \langle b\rangle$, $H_1 = \langle b, c_1\rangle$, $\cdots$, $H_{k-1} = \langle b, c_1, \cdots, c_{k-1}\rangle$. 由于 $[a,b] \notin H_i$, 故 $H_i \ntrianglelefteq G$, $i = 0, 1, \cdots, k-1$. 显然, $|H_i| = p^{i+1}$ 且 $|H_i^G| = |H_iG'| = p^{i+2}$, 其中 $i = 0, 1, \cdots, k-1$. 因此 $\Delta(G) = \{p^2, p^3, \cdots, p^{k+1}\}$, 即 $|\Delta(G)| = k$. □

11.6　非正规子群的正规闭包均包含导群的 p 群

设 G 是有限群, H 是 G 的子群. 明显地, $H \trianglelefteq G$ 当且仅当 $H^G = H$. 于是正规闭包作为子群正规程度的一个度量, 在研究有限群的结构中起着重要作用. 例如, Janko[98] 分类了每个非正规子群 H 的正规闭包在 G 中指数为 p 的 p 群 G, 即 $|G:H^G| = p$ 的 p 群. 进一步地, 张军强等[260] 分类了 G/H^G 循环的 p 群 G. 有趣的是, 这样的 p 群恰是 Janko 在文献 [96] 分类的一类群. 郭秀云等[284] 研究了每个非正规循环子群 H 的正规闭包在 G 中指数为 p^w 的 p 群 G, 特别是, 分类了 $|G:H^G| \leqslant p^2$ 的 p 群. 张军强等[261] 研究了 G/H^G 交换的 p 群 G(称之为 $\mathcal{C}_a$ 群) 并在某种条件下给出了其分类. 吕恒等[141] 研究了每个非正规子群 H 的正规闭包 $H^G = HG'$ 的 p 群 (称为 N_3 群). 显然 N_3 群恰为 $\mathcal{C}_a$ 群. 文献 [141], [261], [284] 分别独立地、从不同角度出发对 $\mathcal{C}_a$ 群进行了研究. 本节介绍该方面的有关结果.

设 G 是有限 p 群. 称 G 为 $\mathcal{C}_c$ 群, 若对 G 的每个非正规子群 H 均有 G/H^G 循环. 称 G 为 $\mathcal{C}_a$ 群, 若对 G 的每个非正规子群 H 均有 G/H^G 交换. 注意到 p^4 阶群均是 $\mathcal{C}_a$ 群. $\mathcal{C}_a$ 群的商群也是 $\mathcal{C}_a$ 群.

首先我们给出 $\mathcal{C}_c$ 群的某些等价条件及分类.

定理 11.6.1 [260]　设 G 是一个非 Dedekind p 群. 则下列条件等价.

(1) 对 G 的任意极小非正规子群 L 都有 G/L^G 循环;

(2) 对 G 的任意非正规子群 H 都有 G/H^G 循环;

(3) $\Phi(G)$ 的任意子群都在 G 中正规且 $d(G) = 2$;

(4) G 的任意给定的一个非正规子群都包含于唯一的一个极大子群中.

证明　(1)⇒(2): 设 H 是 G 的一个非正规子群. 则存在 G 的一个极小非正规子群 L 使得 $L \leqslant H$. 由假设 G/L^G 循环. 由 $L^G \leqslant H^G$ 可得 G/H^G 循环. 于是 (2) 成立.

(2)⇒(3): 设 $K \leqslant \Phi(G)$. 则 $K^G \leqslant \Phi(G)$. 因为 G 非循环, 所以 $G/\Phi(G)$ 非循环. 从而 G/K^G 非循环. 那么 $K \trianglelefteq G$. 于是 $\Phi(G)$ 的所有子群都在 G 中正规. 假设 L 是 G 的一个极小非正规子群. 由引理 11.1.1 得 L 循环. 令 $L = \langle a \rangle$. 因为 $L^G \leqslant LG'$ 且 G/L^G 循环, 所以 G/LG' 循环. 令 $G/LG' = \langle \bar{b} \rangle$. 则 $G = \langle a, b, G' \rangle = \langle a, b \rangle$. 于是 $d(G) = 2$. 结论 (3) 成立.

(3) ⇒(4): 令 M_1 和 M_2 是 G 的两个不同的极大子群. 由 $d(G) = 2$ 可得 $M_1 \bigcap M_2 = \Phi(G)$. 如果 $H \leqslant M_1 \bigcap M_2 = \Phi(G)$, 那么 $H \trianglelefteq G$. 于是结论 (4) 成立.

(4) ⇒(1): 设 L 是 G 的一个极小非正规子群. 那么 L 包含于 G 的一个唯一的极大子群中. 从而 $L\Phi(G)$ 包含于 G 的一个唯一的极大子群中. 注意到 $G/L\Phi(G)$ 初等交换. 由对应定理, $G/L\Phi(G)$ 的阶为 p. 令 $G/L\Phi(G) = \langle \bar{a} \rangle$. 则 $G = \langle a, L, \Phi(G) \rangle =$

$\langle a, L\rangle = \langle a\rangle L^G$. 于是 $G/L^G = \langle \bar{a}\rangle$. 结论 (1) 成立. □

由定理 11.6.1 可知, Janko 在文献 [96] 中所分类的群就是 $\mathcal{C}_c$ 群. 张军强等在文献 [260] 对 $\mathcal{C}_c$ 群的分类给出了一个独立的证明. 下面仅列出分类结果, 证明过程略去.

定理 11.6.2 ([260]) 设 G 是有限 p 群且至少有一个非正规子群. 则 G 是 $\mathcal{C}_c$ 群当且仅当 G 是下列互不同构的群之一.

(Ⅰ) $\mathrm{M}_p(n, m)$ 或 $\mathrm{M}_p(n, m, 1)$.

(Ⅱ) 阶 $\geqslant 2^4$ 的极大类 2 群.

(Ⅲ) 阶为 2^{n+2} 非亚循环群, $n \geqslant 3$:

(Ⅲ-1) $\langle a, b, c \mid a^{2^n} = b^2 = 1, [a, b] = c, c^2 = a^{-4}, [c, a] = 1, [c, b] = c^{-2}\rangle$;

(Ⅲ-2) $\langle a, b, c \mid a^{2^n} = 1, b^2 = a^{2^{n-1}}, [a, b] = c, c^2 = a^{-4}, [c, a] = 1, [c, b] = c^{-2}\rangle$;

(Ⅲ-3) $\langle a, b, c \mid a^{2^n} = b^4 = 1, [a, b] = c, c^2 = a^{-4}, [c, a] = 1, [c, b] = c^{-2}\rangle$.

(Ⅳ) 阶为 2^{n+2} 亚循环群, $n \geqslant 3$:

(Ⅳ-1) $\langle a, b \mid a^{2^n} = b^4 = 1, [a, b] = a^{-2}\rangle$;

(Ⅳ-2) $\langle a, b \mid a^{2^n} = b^4 = 1, [a, b] = a^{-2+2^{n-1}}\rangle$.

下面介绍 $\mathcal{C}_a$ 群的有关结果. 对于 $\mathcal{C}_a$ 群首先有下列等价命题.

引理 11.6.3 ([261]) 设 G 是一个非 Dedekind p 群. 那么下列条件等价.

(1) 对 G 的任意极小非正规子群 L 都有 G/L^G 交换;

(2) 对 G 的任意非正规子群 H 都有 G/H^G 交换;

(3) 对 G 的任意非正规子群 H 都有 $H^G = HG'$;

(4) 对 G 的任意正规子群 K 有 $G' \leqslant K$ 或 K 的所有子群在 G 中正规.

证明 设 H 是 G 的一个非正规子群, K 是 G 的一个正规子群.

(1) $\Rightarrow$(2): 存在 $L \leqslant H$ 使得 L 是 G 的一个极小非正规子群. 由假设得 G/L^G 交换. 从而 G/H^G 交换.

(2) $\Rightarrow$(3): 因为 G/H^G 交换, 所以 $G' \leqslant H^G$. 从而 $HG' \leqslant H^G$. 注意到 $HG' \trianglelefteq G$. 于是 $H^G = HG'$.

(3) $\Rightarrow$(4): 如果存在 $N \leqslant K$ 使得 $N \ntrianglelefteq G$, 则 $G' \leqslant N^G \leqslant K$. 从而 (4) 成立.

(4) $\Rightarrow$(1): 设 L 是 G 的一个极小非正规子群. 则 $L \leqslant L^G \trianglelefteq G$. 从而 $G' \leqslant L^G$. 于是 G/L^G 交换. □

赵立博等[284] 研究了每个非正规循环子群 H 的正规闭包在 G 中指数为 p^w 的 p 群 G. 他们记这样的 p 群为 $C(p^w)$ 群. 特别是, 分类了 $C(p^2)$ 群. 容易看出, $C(p^w)$ 群的商群是 $C(p^w)$ 群. 由引理 11.6.3 可知, $C(p^2)$ 群是 $\mathcal{C}_a$ 群.

引理 11.6.4 ([284]) 设 G 是非 Dedekind p 群, $p > 2$. 若 G 是一个 $\mathcal{C}_a$ 群, 则

(1) 若 G' 循环, 则 $|G'| = p$;

(2) 若 G' 的每个循环子群在 G 中正规, 则 $\exp(G') = p$ 且 $G' \leqslant Z(G)$.

证明 (1) 因为 G' 循环, 故 G 正则. 从而存在 a 和 b 使得 $[a,b]=c$, $\langle a\rangle\bigcap\langle c\rangle=1$ 且 $G'=\langle c\rangle$. 若 $o(a)=p$, 由

$$1=[a^p,b]=[a,b]^p[a,b,a]^{\binom{p}{2}}[a,b,a,a]^{\binom{p}{3}}\cdots=c^{p(1+kp)}$$

推出 $c^p=1$. 若 $o(a)\geqslant p^2$ 且 $o(c)>p$, 则

$$\langle a^p\rangle\ntrianglelefteq G\quad 且\quad \langle a^p\rangle^G=\langle a^p,[a^p,G]\rangle\leqslant\langle a^p,c^p\rangle=\langle a^p\rangle\Phi(G').$$

于是

$$G'=G'\bigcap\langle a^p\rangle^G\leqslant(G'\bigcap\langle a^p\rangle)\Phi(G').$$

从而 $G'\leqslant\langle a^p\rangle$. 这与 $\langle a^p\rangle\ntrianglelefteq G$ 矛盾. 故 $|G'|=p$.

(2) 因为 G' 是 Dedekind p 群, 故 G' 交换. 令 $G'=\times_{i=1}^{s}U_i$, 其中 U_i 循环, $i=1,2,\cdots,s$. 令 $T_j=\times_{i\neq j}U_i$. 则 (G/T_j) 非交换且 $(G/T_j)'$ 循环. 由 (1) 得 $|(G/T_j)'|=p$. 于是 $\exp(G')=p$ 且 $[G,G']\leqslant\bigcap_{j=1}^{s}T_j=1$. 因而 $G'\leqslant Z(G)$. □

定理 11.6.5 [261] *设 G 是一个有限非 Dedekind p 群, 其中 $p>2$. 若 G 是 $\mathcal{C}_a$ 群, 则*

(1) *G' 有一个极大子群 M 使得 $M\leqslant Z(G)$ 且 M 初等交换;*

(2) *$c(G)\leqslant 3$;*

(3) *G' 初等交换;*

(4) *$\mho_1(G)\leqslant Z(G)$.*

证明 (1) 由 [247] 中的推论 2.2.6 可得, G' 有一个极大子群 M 使得 $M\trianglelefteq G$. 又由引理 11.6.3(4) 得, M 的所有子群都在 G 中正规. 因为 $p>2$, 故 M 交换. 不妨设

$$M=\langle d_1\rangle\times\cdots\times\langle d_s\rangle,\quad o(d_1)\geqslant\cdots\geqslant o(d_s).$$

令 $\overline{G}=G/\langle d_2,\cdots,d_s\rangle$. 注意到 $\exp(M)=o(d_1)=o(\bar{d_1})$. 若 $o(\bar{d_1})=p$, 则 M 初等交换且 $M\leqslant Z(G)$. 下证 $o(\bar{d_1})=p$.

若 $\overline{G}'$ 的所有循环子群都在 $\overline{G}$ 中正规, 由引理 11.6.4(2) 可得 $\exp(\overline{G}')=p$. 于是 $o(\bar{d_1})=p$. 结论成立.

若存在 $\overline{G}'$ 的循环子群 $\overline{H}$ 使得 $\overline{H}$ 在 $\overline{G}$ 中不正规, 令 $\overline{H}=\langle\bar{x}\rangle$, 则 $\overline{G}'=\langle\overline{M},\bar{x}\rangle$ 且 $\langle\bar{x}\rangle<\overline{G}'$. 因为 $\overline{M}=\langle\bar{d_1}\rangle$, 所以 $|\overline{G}':\langle\bar{d_1}\rangle|=p$ 且 $\langle\bar{d_1}\rangle\trianglelefteq\overline{G}$. 从而 $[\langle\bar{x}\rangle,\overline{G}]\leqslant\langle\bar{d_1}\rangle$. 若 $[\langle\bar{x}\rangle,\overline{G}]<\langle\bar{d_1}\rangle$, 则 $[\langle\bar{x}\rangle,\overline{G}]\leqslant\Phi(\overline{G}')$. 故 $\langle\bar{x}\rangle^{\overline{G}}=\langle\bar{x}\rangle[\langle\bar{x}\rangle,\overline{G}]\leqslant\langle\bar{x}\rangle\Phi(\overline{G}')$. 易证 $\overline{G}$ 是一个 $\mathcal{C}_a$ 群. 从而 $\overline{G}'\leqslant\langle\bar{x}\rangle^{\overline{G}}\leqslant\langle\bar{x}\rangle$, 矛盾. 所以 $[\langle\bar{x}\rangle,\overline{G}]=\langle\bar{d_1}\rangle$. 于是存在 $\bar{g}$ 使得 $[\bar{x},\bar{g}]=\bar{d_1}^{\,j}$, 其中 $(p,j)=1$. 从而 $\overline{G}_3=\langle\bar{d_1}\rangle$, $\overline{G}_4\leqslant\langle\bar{d_1}^{\,p}\rangle$ 且 $\overline{G}_5\leqslant\langle\bar{d_1}^{\,p^2}\rangle$. 因为 $\bar{x}^p=\bar{1}$ 且 $\langle\bar{d_1}\rangle\trianglelefteq\overline{G}$, 由命题 1.1.9 可得

$$\bar{1}=[\bar{x}^p,\bar{g}]=[\bar{x},\bar{g}]^p[\bar{x},\bar{g},\bar{x}]^{\binom{p}{2}}\cdots=[\bar{x},\bar{g}]^p\bar{d_1}^{\,kp^2}=\bar{d_1}^{\,jp+kp^2}.$$

从而 $o(\bar{d}_1)=p$. 于是结论成立.

(2) 注意到 $c(G/M)=2$ 且 $M\leqslant Z(G)$, 可得 (2) 成立.

(3) 因为 M 是 G' 的极大子群且 $M\leqslant Z(G)$, 故 G' 交换. 若 $\Omega_1(G')\leqslant Z(G)$, 则存在 $d\in G'$ 使得 $G'=\langle d\rangle\times N$, 其中 $N\leqslant M\leqslant Z(G)$. 从而 $(G/N)'$ 循环. 由 (1) 的证明过程可得 $o(d)=|(G/N)'|=p$. 于是 G' 初等交换. 若存在 $x\in\Omega_1(G')$ 使得 $x\notin Z(G)$, 则 $G'=\langle M,x\rangle$. 从而 G' 初等交换.

(4) 对任意的 $a,b\in G$, 由 (2),(3) 和命题 1.1.9 可得

$$[a^p,b]=[a,b]^p[a,b,a]^{\binom{p}{2}}=1.$$

从而 $a^p\in Z(G)$. 于是 $\mho_1(G)\leqslant Z(G)$. □

吕恒等在文献 [141] 中也得到了定理 11.6.5 中的结论 (2)—(4), 这里给出的证明采用文献 [261] 的证明.

定理 11.6.6 [261] 设 G 是有限非 Dedekind p 群, 其中 $p>2$. 若 G 是 $\mathcal{C}_a$ 群且 $c(G)=3$, 则下列结论成立.

(1) 若 $|G_3|=p$, 则 $Z(G)$ 循环;

(2) $d(G)\leqslant 3$;

(3) 若 $|G|\geqslant p^6$, 则 $|G_3|=p$.

证明 (1) 因为 $c(G)=3$, 故存在 $h\in G'$ 使得 $h\notin Z(G)$. 由定理 11.6.5(3) 可得 $G'=\langle M\rangle\times\langle h\rangle$, 其中 $o(h)=p$, M 为 G' 的初等交换极大子群且 $M\leqslant Z(G)$. 于是对任意的 $g\in G$ 都有 $[h,g]\in M\leqslant Z(G)$. 对任意的 $1\neq z\in Z(G)$, 若 $G_3\nleqslant\langle z\rangle$, 则 $\langle hz\rangle\ntrianglelefteq G$. 由假设可得 $h\in G'\leqslant\langle hz\rangle^G=\langle hz,G_3\rangle$. 令 $h=(hz)^ix$, 其中 $x\in G_3$ 且 $i\in\{0,1,\cdots,p-1\}$. 则 $h^{1-i}=z^ix\in\langle h\rangle\bigcap Z(G)=1$. 从而 $i=1$. 所以 $z=x^{-1}\in G_3$. 于是 $\langle z\rangle=G_3$, 矛盾. 这说明对任意的 $z\in Z(G)$ 都有 $G_3\leqslant\langle z\rangle$. 从而 $\Omega_1(Z(G))=G_3$. 故 $Z(G)$ 循环.

(2) 若 $|G_3|\geqslant p^2$, 则存在 $N\leqslant G_3$ 使得 $|(G/N)_3|=p$. 从而 $d(G)=d(G/N)$. 于是只需要证明, 若 $|G_3|=p$, 则 $d(G)\leqslant 3$.

设 $|G_3|=p$. 则由 (1) 可得 $Z(G)$ 循环. 令 $Z(G)=\langle z\rangle$. 由定理 11.6.5(4) 可得, $\mho_1(G)\leqslant Z(G)$ 且 $G_2\cong \mathrm{E}_{p^2}$. 从而 $G/Z(G)$ 方次数为 p 且 $|(G/Z(G))'|=|\langle\bar{h}\rangle|=p$. 由定理 10.1.2 可得

$$G/Z(G)\cong \mathrm{M}_p(1,1,1)*\mathrm{M}_p(1,1,1)*\cdots*\mathrm{M}_p(1,1,1)\times \mathrm{E}_{p^t}.$$

令

$$G/Z(G)=\langle\bar{a}_1,\bar{b}_1\rangle*\cdots*\langle\bar{a}_s,\bar{b}_s\rangle\times\langle\bar{c}_1\rangle\times\cdots\times\langle\bar{c}_t\rangle,$$

其中对任意的 $i\in\{1,2,\cdots,s\}$ 都有 $\langle\bar{a}_i,\bar{b}_i\rangle\cong \mathrm{M}_p(1,1,1)$ 且对任意的 $j\in\{1,2,\cdots,t\}$ 都有 $o(\bar{c}_j)=p$. 若 $s\geqslant 2$, 则存在 $i\neq j$ 使得 $\langle[\bar{a}_i,\bar{b}_i]\rangle=\langle[\bar{a}_j,\bar{b}_j]\rangle=\langle\bar{h}\rangle$. 因为

$[a_i,a_j],[a_i,b_j]\in Z(G)$, 所以

$$[a_i,[a_j,b_j]]=[a_i,a_j^{-1}b_j^{-1}a_jb_j]=[a_i,a_j]^{-1}[a_i,b_j]^{-1}[a_i,a_j][a_i,b_j]=1.$$

从而 $[a_i,h]=1$. 类似地, 可得 $[b_i,h]=1$. 由 i 的任意性可得 $h\in Z(G)$, 矛盾. 所以 $s=1$, 即 $G/Z(G)\cong \mathrm{M}_p(1,1,1)\times \mathrm{E}_{p^t}$. 令

$$o(c_k)=\max\{o(c_1),o(c_2),\cdots,o(c_t)\}.$$

若 $t\geqslant 2$, 则存在 $l\neq k$ 使得 $c_l^p\in\langle c_k^p\rangle$. 令 $c_l^p=c_k^{ip}$. 则 $(c_lc_k^{-i})^p=1$ 且 $c_lc_k^{-i}\notin Z(G)$. 于是 $\langle c_lc_k^{-i}\rangle$ 是 G 的一个 p 阶正规子群. 从而

$$h\in G'\leqslant \langle c_lc_t^{-i}\rangle^G=\langle c_lc_t^{-i},[\langle c_lc_t^{-i}\rangle,G]\rangle\leqslant\langle c_lc_t^{-i},G_3\rangle,$$

矛盾. 于是 $t\leqslant 1$ 且 $G=\langle a_1,b_1\rangle$ 或者 $G=\langle a_1,b_1,c_1\rangle$.

(3) 假设 $|G|\geqslant p^6$. 若 $|G_3|=p^2$, 则由定理 11.6.5(3) 可得 $G_3\cong \mathrm{E}_{p^2}$. 于是对任意的 $z\in Z(G)$ 都有 $\langle hz\rangle\ntrianglelefteq G$. 从而 $z=x^{-1}\in G_3$. 由 z 的任意性可得 $Z(G)\leqslant G_3$. 于是 $Z(G)=G_3$. 令

$$Z(G)=G_3=\langle x_1,x_2\rangle=Z(G)\cong \mathrm{E}_{p^2}\quad 且\quad G'=\langle h,x_1,x_2\rangle\cong \mathrm{E}_{p^3}.$$

从而存在 $a,b\in G$ 使得 $[a,b]=h$. 考虑 G/G_3. 由定理 11.6.5(4) 可得, $\mho_1(G)\leqslant Z(G)=G_3$ 且 $\Phi(G)=G'$. 于是 $|G/\Phi(G)|=|G/G'|\geqslant p^3$. 从而 $d(G)\geqslant 3$. 由 (2) 可得 $d(G)=3$. 那么 $d(G/G_3)=3$. 注意到 $|G'/G_3|=p$ 且 $\mho_1(G)\leqslant Z(G)$, 可得 G/G_3 的方次数为 p 且 $|(G/G_3)'|=p$. 由定理 10.1.2 可得 $G/G_3\cong \mathrm{M}_p(1,1,1)\times \mathrm{C}_p$. 于是存在 $d\in G$ 使得 $G=\langle a,b,d\rangle$ 且 $G/G_3=\langle\bar{a},\bar{b}\rangle\times\langle\bar{d}\rangle$. 从而 $[d,a],[d,b]\in G_3$. 那么 $[d,h]=[d,[a,b]]=1$. 注意到 $d^p\in Z(G)$, 可得 $h\notin\langle d\rangle^G=\langle d,[d,a],[d,b]\rangle$. 这意味着 $\langle d\rangle\trianglelefteq G$, 所以对任意的 $g\in G$ 都有 $[d,g]\in\langle d^p\rangle$. 因为 $h\notin\langle dh\rangle^G\leqslant\langle dh,G_3\rangle$, 故 $\langle dh\rangle\trianglelefteq G$. 从而对任意的 $g\in G$ 都有 $[dh,g]\in\langle (dh)^p\rangle=\langle d^p\rangle$. 由此得 $[h,g]\in\langle d^p\rangle$. 于是

$$G_3=[G_2,G]=\langle [h,g]\mid g\in G\rangle\leqslant\langle d^p\rangle\cong \mathrm{C}_p.$$

矛盾. 故 $|G_3|=p$. □

下面的例子告诉我们: 存在 p^5 阶的 $\mathcal{C}_a$ 群使得 $c(G)=3$ 且 $|G_3|=p^2$.

例 11.6.7 令 $G=\langle a,b,c\mid a^{3^2}=b^{3^2}=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^3\rangle$. 易得 G 是一个 3^5 阶的 $\mathcal{C}_a$ 群, $d(G)=2=\log_p|G'|-1$ 且 $G_3=Z(G)=\langle a^3,b^3\rangle\cong \mathrm{E}_{3^2}$.

定理 11.6.8 ([261]) 设 G 是一个有限非 Dedekind$p$ 群, 其中 $p>2$. 若 G 是一个 $\mathcal{C}_a$ 群且 $c(G)=2$, 则 $\Phi(G)\leqslant Z(G)$ 且 $d(G)\geqslant\log_p|G'|$.

证明 由定理 11.6.5(4) 可得 $\mho_1(G) \leqslant Z(G)$. 因为 $c(G)=2$, 故 $G' \leqslant Z(G)$. 从而 $\Phi(G) \leqslant Z(G)$. 设 $H=\langle h\rangle$ 是 G 的一个循环非正规子群. 因为 $\Phi(G) \leqslant Z(G)$, 故 $h \notin \Phi(G)$. 令 $d(G)=t+1$ 且 $G=\langle h, a_1, a_2, \cdots, a_t\rangle$. 因为 G 是一个 $\mathcal{C}_a$ 群, 故

$$G' \leqslant H^G=\langle h,[h, g] | g \in G\rangle=\langle h,[h, a_1], \cdots,[h, a_t]\rangle.$$

由定理 11.6.5(3) 可得 $\exp(G')=p$. 从而

$$|G'| \leqslant |\Omega_1(\langle h,[h, a_1], \cdots,[h, a_t]\rangle)| \leqslant p^{t+1}=p^{d(G)}.$$

于是 $d(G) \geqslant \log_p |G'|$. □

定理 11.6.9 ([261]) 假设 G 是一个非 Dedekind 的 $\mathcal{C}_a$ 群且 $c(G)=2$, $d(G)=\log_p |G'|$, 其中 $p>2$. 则存在 G 的一个极小生成系 $\{a_1, a_2, \cdots, a_d\}$ 使得

$$a_1^{p^{n_1}}=a_2^{p^{n_2}}=\cdots=a_d^{p^{n_d}}=1, \quad n_1 \geqslant n_2 \geqslant \cdots \geqslant n_d \geqslant 2$$

且

(1) $\langle a_i\rangle \ntrianglelefteq G$ 且对任意不同的 $i, j \in\{1,2, \cdots, d\}$ 都有 $[a_i, a_j] \neq 1$.

(2) 对任意的 $i \in\{1,2, \cdots, d\}$ 都有 $G'=\langle a_i^{p^{n_i-1}},[a_i, a_1],[a_i, a_2], \cdots,[a_i, a_d]\rangle$. 特别地, $G'=\langle a_1^{p^{n_1-1}}\rangle \times\langle a_2^{p^{n_2-1}}\rangle \times \cdots \times\langle a_d^{p^{n_d-1}}\rangle=\Omega_1(G) \cong \mathrm{E}_{p^d}$.

证明 由定理 11.6.5(3) 可得 $\exp(G')=p$. 再由 [247] 中的推论 4.2.2 可得 G 为 p 交换的. 令 $G / G'=\langle\bar{b}_1\rangle \times\langle\bar{b}_2\rangle \times \cdots \times\langle\bar{b}_d\rangle$ 满足关系

$$\bar{b}_1^{p^{m_1}}=\bar{b}_2^{p^{m_2}}=\cdots=\bar{b}_d^{p^{m_d}}=\bar{1},$$

其中 $m_1 \geqslant m_2 \geqslant \cdots \geqslant m_d \geqslant 1$. 于是 $G=\langle b_1, b_2, \cdots, b_d\rangle$. 令 $a_1=b_1$. 对任意的 $i \geqslant 2$, 若 $b_i=\prod_{t=1}^{i-1} b_t^{i_t p^{m_t}}$, 则通过令 $a_i=b_i \prod_{t=1}^{i-1} b_t^{-i_t p^{m_t-m_i}}$ 可得 $a_i^{p^{m_i}}=1$. 若否, 则通过令 $a_i=b_i$ 可得 $a_i^{p^{m_i+1}}=1$. 于是可得 $G=\langle a_1, a_2, \cdots, a_d\rangle$ 满足关系

$$a_1^{p^{n_1}}=a_2^{p^{n_2}}=\cdots=a_d^{p^{n_d}}=1.$$

不失一般性, 可令 $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_d \geqslant 1$.

首先证明若 $\langle a_i\rangle \ntrianglelefteq G$, 则对任意的 $i \in\{1,2, \cdots, d\}$ 都有

$$G'=\langle a_i^{p^{n_i-1}},[a_i, a_1],[a_i, a_2], \cdots,[a_i, a_d]\rangle,$$

且对任意的 $j \neq i$ 都有 $[a_i, a_j] \neq 1$. 事实上, 因为 G 是一个 $\mathcal{C}_a$ 群, 所以

$$G' \leqslant \Omega_1(\langle a_i\rangle^G)=\langle a_i^{p^{n_i-1}},[a_i, a_1],[a_i, a_2], \cdots,[a_i, a_d]\rangle.$$

由定理 11.6.5(3) 可得 $\exp(G')=p$. 故对任意的 i 和 j 都有 $o([a_i,a_j])\leqslant p$. 由假设可得 $G'=\Omega_1(\langle a_i\rangle^G)$. 于是对任意的 $j\neq i$ 都有 $[a_i,a_j]\neq 1$.

下面证明对任意的 i 都有 $\langle a_i\rangle\ntrianglelefteq G$. 若否, 则存在 i 使得 $\langle a_i\rangle\trianglelefteq G$. 于是对任意的 $j\in\{1,2,\cdots,d\}$ 都有 $[a_i,a_j]\in\langle a_i^{p^{n_i-1}}\rangle$. 令 t 是使得 $[a_i,a_t]\neq 1$ 的最大值. 则 $[a_i,a_j]\in\langle[a_i,a_t]\rangle$. 令 $[a_i,a_j]=[a_i,a_t]^{-x_j}$, $1\leqslant j\leqslant t-1$. 则

$$[a_i,a_1a_t^{x_1}]=[a_i,a_2a_t^{x_2}]=\cdots=[a_i,a_{t-1}a_t^{x_{t-1}}]=1.$$

从而 $\langle a_sa_t^{x_s}\rangle\trianglelefteq G$, 其中 $s\in\{1,2,\cdots,t-1\}$. 对任意两个不同的 $s_1,s_2\in\{1,2,\cdots,t-1\}$, 因为 G 是 p 交换的且 $o(a_t)\leqslant\min\{o(a_{s_1}),o(a_{s_2})\}$, 故 $\langle a_{s_1}a_t^{x_{s_1}}\rangle\bigcap\langle a_{s_2}a_t^{x_{s_2}}\rangle=1$. 于是

$$[a_{s_1}a_t^{x_1},a_{s_2}a_t^{x_1}]\in\langle a_{s_1}a_t^{x_1}\rangle\bigcap\langle a_{s_2}a_t^{x_1}\rangle=1.$$

类似可得对任意 $s_1\in\{1,2,\cdots,t-1\}$ 和两个不同的 $s_3,s_4\in\{t+1,t+2,\cdots,d\}$ 都有

$$[a_{s_1}a_t^{x_1},a_{s_3}]=[a_{s_3},a_{s_4}]=1.$$

因为

$$G=\langle a_1,a_2,\cdots,a_d\rangle=\langle a_1a_t^{x_1},a_2a_t^{x_1},\cdots,a_{t-1}a_t^{x_{t-1}},a_t,\cdots,a_d\rangle$$

且 $c(G)=2$, 由此可得

$$G'=\langle[a_1a_t^{x_1},a_t],\cdots,[a_{t-1}a_t^{x_1},a_t],[a_{t+1},a_t],\cdots,[a_d,a_t]\rangle.$$

注意到 $\exp(G')=p$, 可得 $|G'|\leqslant p^{d-1}$. 与假设矛盾. □

命题 11.6.10 [261]　*设 K 是 $\mathcal{C}_a$ 群且满足 $c(K)=2$ 和 $|K'|=p^m$, H 是阶为 p^n 的初等交换群. 则 $G=K\times H$ 是 $\mathcal{C}_a$ 群, 且满足 $d(G)\geqslant m+n$ 和 $|G'|=p^m$.*

证明　令 $L=\langle a\rangle$ 是 G 的一个循环子群. 则 $a=xz$, 其中 $x\in K$ 且 $z\in H$. 注意到对任意的 $g\in G$ 和 $\langle x^p\rangle=\langle(xz)^p\rangle$ 都有 $[xz,g]=[x,g]$. 由此可得 $\langle a\rangle\trianglelefteq G$ 当且仅当 $\langle x\rangle\trianglelefteq K$. 若 $L\ntrianglelefteq G$, 则 $\langle x\rangle\ntrianglelefteq K$. 因为 $K\in\mathcal{C}_a$, 故 $K'\leqslant\langle x\rangle^K=\langle x,[\langle x\rangle,K]\rangle$. 注意到 $c(K)=2$. 于是 $K'\leqslant Z(K)$ 且 $x\notin K'$. 从而

$$G'=K'\leqslant\langle x^p\rangle[\langle x\rangle,K]=\langle(xz)^p\rangle[\langle xz\rangle,G]\leqslant\langle xz\rangle^G.$$

于是 G 是一个 $\mathcal{C}_a$ 群. □

命题 11.6.10 告诉我们, 存在生成元的个数和导群的阶均任意大的 $\mathcal{C}_a$ 群.

下面分类一类特殊的 $\mathcal{C}_a$ 群, 即 $C(p^2)$ 群. 很清楚, 阶 $\leqslant p^4$ 的 p 群都是 $C(p^2)$ 群. 因而可设 $C(p^2)$ 群的阶 $\geqslant p^5$. 若 $C(p^2)$ 群的阶为 p^5, 利用 $p^5(p\geqslant 5)$ 阶群的分类[270] 以及 Magma[37] 对小群库中的 3^5 阶群检验即得所有的 $C(p^2)$ 群, 参看 [284] 中的定理 2.4. 下设 $C(p^2)$ 群的阶 $\geqslant p^6$.

定理 11.6.11 ([284]) 设 G 是非 Dedekind 的 $C(p^2)$ 群, $p>2$ 且其阶至少为 p^6. 则 $G\cong\langle a,b\mid a^{p^3}=b^{p^3}=1,[a,b]=a^{p^2}\rangle$ 或 $\langle a,b,c\mid a^{p^2}=b^{p^2}=c^{p^2}=1,[a,c]=a^p,[b,c]=b^p,[a,b]=1\rangle$.

证明 首先, 我们分类 p^6 阶的非 Dedekind 的 $C(p^2)$ 群 G. 易知 $d(G)\leqslant 3$. 若 $G=\langle a,b\rangle$ 且 $|G'|=p^4$, 则 $|G/N|=p^5$ 且 $(G/N)'=p^3$, 其中 $N\leqslant G'\bigcap Z(G)$ 且 $|N|=p$. 由 [284] 中的定理 2.4 可知, G/N 同构于 [284] 中的定理 2.4 的群 (8)—(14) 或 (24)—(30). 这些群均有 $|(G/N)_3|=p^2$, 从而 $|G_3|=p^3$. 这与定理 11.6.6(3) 矛盾. 于是 $|G'|\leqslant p^3$ 且由假设可知, G' 的每个循环子群在 G 中正规. 由引理 11.6.4(2) 可知, $c(G)=2$ 且 $\exp(G')=p$. 若 $d(G)=2$, 则 $|G'|=p$. 又由定理 1.7.7 可知, G 内交换. 再由定理 1.7.10 可得, $G=\langle a,b\mid a^{p^3}=b^{p^3}=1,[a,b]=a^{p^2}\rangle$.

设 $d(G)=3$. 则 $|G'|\leqslant p^3$. 由引理 11.6.4(2) 可得, $\exp(G')=p$ 且 $c(G)=2$. 因而 G 正则. 不妨设 $G=\langle a,b,c\rangle$, 其中 a,b,c 是 G 的某个唯一性基底且满足 $o(a)\geqslant o(b)\geqslant o(c)$.

若 $G'\cong \mathrm{C}_p$, 由于对 G 的每个非正规循环子群 H 均有 $H^G=HG'$, 故由假设可得, 阶 $\leqslant p^2$ 的循环子群在 G 中正规. 从而 $\exp(G)\geqslant p^3$. 若 $\exp(G)=p^4$, 则 (a,b,c) 是 G 的一组唯一性基底且满足 $o(a)=p^4$ 和 $o(b)=o(c)=p$. 而 $\langle b\rangle$ 和 $\langle c\rangle$ 的正规性隐含着 G 交换, 矛盾. 清楚地, $\exp(G)\leqslant p^4$. 于是 $\exp(G)=p^3$. 在这种情形下, (a,b,c) 是 G 的一组唯一性基底且满足 $o(a)=p^3,o(b)=p^2$ 和 $o(c)=p$. 因为 $c\in Z(G)$ 且 $\langle b\rangle\trianglelefteq G$, 由 $G'\cong\mathrm{C}_p$ 可知, $[a,b]=b^{pi}$, 其中 $(i,p)=1$. 由此可得 $[a^pb,a]\notin\langle a^pb\rangle$, 这与 $\langle a^pb\rangle\trianglelefteq G$ 矛盾.

若 $G'\cong\mathrm{C}_p^3$, 则 a,b,c 中任何一个的阶不是 p. 事实上, 不妨设 $o(a)=p$ 且 $\langle a\rangle\trianglelefteq G$, 则 $\langle a\rangle\leqslant Z(G)$, 因而 $G'=\langle[a,b],[a,c],[b,c]\rangle=\langle[b,c]\rangle$, 矛盾. 若 $o(a)=p$ 且 $\langle a\rangle\ntrianglelefteq G$, 则 $p^2\geqslant|G/\langle a\rangle^G|=|G/\langle a,[a,b],[a,c]\rangle|=p^3$, 又一个矛盾. 于是

$$o(a)=o(b)=o(c)=p^2 \quad 且 \quad \mho_1(G)=G'=\Phi(G)=Z(G)\cong\mathrm{C}_p^3.$$

由 p^6 阶群的分类 [95] 可知, G 是下列群之一.

(A) $\langle a,b,c\mid a^{p^2}=b^{p^2}=c^{p^2}=1,[a,b]=c^p,[b,c]=b^p,[c,a]=a^{-p}\rangle$;

(B) $\langle a,b,c\mid a^{p^2}=b^{p^2}=c^{p^2}=1,[a,b]=c^p,[b,c]=a^p,[c,a]=b^p\rangle$.

清楚地, 对于群 (A), $\langle b\rangle\ntrianglelefteq G$ 且 $G'\nleqslant\langle b\rangle^G$. 于是群 (A) 不满足假设. 设 G 是群 (B). 断言: 存在 $i,j\in\mathrm{F}_p$ 使得 $i^2+j^2\equiv p-1\pmod p$. 事实上, 令

$$S=\{i^2\mid i\in\mathrm{F}_p\} 且 T=\{1-p-j^2\mid j\in\mathrm{F}_p\}.$$

则 $|S|=|T|=\dfrac{p+1}{2}$. 故 $p=|\mathrm{F}_p|<|S|+|T|$. 因而存在 $i,j\in\mathrm{F}_p$ 使得 $i^2+j^2\equiv p-1\pmod p$. 于是存在满足条件 $i^2+j^2\equiv p-1\pmod p$ 的子群 $\langle ab^ic^j\rangle\ntrianglelefteq G$ 使得 $\mathrm{C}_p^3\cong G'\leqslant\mho_1(G)\bigcap\langle ab^ic^j\rangle^G\cong\mathrm{C}_p^2$, 矛盾.

现在我们讨论剩余的情况: $G' \cong C_p^2$. 显而易见, G 的每个 p 阶子群在 G 中正规. 由上述的论证可得, $o(a) = o(b) = o(c) = p^2$. 因而可设 $G' = \langle a^p, b^p \rangle$. 若 $\langle a \rangle \ntrianglelefteq G$, 则 $p^3 = |G/\langle a, b^p \rangle| = |G/\langle a \rangle^G| \leqslant p^2$, 矛盾. 于是 $\langle a \rangle \trianglelefteq G$ 且 $[a, c] = a^{ip}$. 类似地, $\langle b \rangle \trianglelefteq G$ 且 $[b, c] = b^{jp}$. 于是 $[a, b] \in \langle a \rangle \bigcap \langle b \rangle = 1$. 因为 $(ij, p) = 1$ 且 $\langle ab \rangle$ 的循环子群在 G 中正规, 再由 $[ab, c] = a^{ip}b^{jp} \in \langle ab \rangle$ 可得, $i \equiv j \pmod p$. 令 k 是满足 $ik \equiv 1 \pmod p$ 的整数且 $c_1 = c^k$. 则 $G = \langle a, b, c_1 \rangle$ 就是定理中的第二个群.

最后证明不存在阶 $\geqslant p^7$ 的非 Dedekind 的 $C(p^2)$ 群. 若否, 设 G 是这样的群, 具有阶 p^n, $n \geqslant 7$. 若 $|G'| = p$, 则 G 正则且阶 $\leqslant p^{n-4}$ 的每个子群在 G 中正规. 于是存在 $a, b \in G$ 且是 G 的一组唯一性基底使得 $o(a) = p^i, o(b) = p^j$ 且 $G' = \langle [a, b] \rangle \leqslant \langle b \rangle$, 其中 $i \geqslant n-3$ 且 $j \leqslant 3$. 现在 $|\langle a^{p^{i-j}} b \rangle| = p^j$. 然而, $\langle a^{p^{i-j}} b \rangle \ntrianglelefteq G$. 矛盾. 因而 $|G'| > p$. 令 N 是 G 的满足 $N \leqslant G' \bigcap Z(G)$ 的极小正规子群. 则 $G/N \in C(p^2)$, $|G/N| = p^{n-1}$ 且 $|(G/N)'| = |G'|/p$. 由上述论证及归纳可知, 只需证不存在阶为 p^7 且满足 $|G'| > p$ 的 $C(p^2)$ 群. 若否, 令 $N = \langle x \rangle$. 则 $\overline{G} = G/N$ 是定理中的群之一. 若

$$\overline{G} = \langle \bar{a}, \bar{b} | \bar{a}^{p^3} = \bar{b}^{p^3} = 1, [\bar{a}, \bar{b}] = \bar{a}^{p^2} \rangle,$$

则 $|G'| = p^2$. 不妨设 $a^{p^3} = x$. 令 $b^{p^3} = x^i$. 则 $[a, b^p a^{-ip}] = x$ 且 $|\langle b^p a^{-ip} \rangle| = p^2$. 但是 $\langle b^p a^{-ip} \rangle \ntrianglelefteq G$, 这与阶 $\leqslant p^2$ 的每个循环子群在 G 中正规矛盾. 若

$$\overline{G} = \langle \bar{a}, \bar{b}, \bar{c} | \bar{a}^{p^2} = \bar{b}^{p^2} = \bar{c}^{p^2} = 1, [\bar{a}, \bar{b}] = 1, [\bar{a}, \bar{c}] = \bar{a}^p, [\bar{b}, \bar{c}] = \bar{b}^p \rangle,$$

则 $|G'| = p^3$. 不妨设 $a^{p^2} = x$. 令 $c^{p^2} = x^i$. 则 $[a, c^p a^{-ip}] = x$ 且 $|\langle c^p a^{-ip} \rangle| = p$. 然而, $\langle c^p a^{-ip} \rangle \ntrianglelefteq G$, 这又与阶为 p 的每个循环子群在 G 中正规矛盾. □

定理 11.6.12 ([284]) *设 G 是非 Dedekind 的 $C(p^w)$ 群, $p > 2$. 若对 G 的每个非循环正规子群 H 均有 $G' \leqslant H^G$, 则 $c(G) \leqslant 3$, $\exp(G_3) \leqslant p$ 且 $|G| \leqslant p^{4w+4}$.*

证明　首先证明: $\exp(G_3) \leqslant p$ 且 $c(G) \leqslant 3$. 事实上, 由引理 11.6.4(2) 不妨设 G' 有一个循环子群 H 使得 $H \ntrianglelefteq G$. 若 G_3 循环, 由 $[H, G] \leqslant G_3$ 推出 $H^G = H[H, G]$. 若 $[H, G] < G_3$, 则 $G_3 = G_3 \bigcap H[H, G] = (G_3 \bigcap H)[H, G] = G_3 \bigcap H$, 这就有 $G_3 \leqslant H$, 从而 $H = H^G \trianglelefteq G$, 矛盾. 因而 $G_3 = [H, G]$ 且存在 $g \in G$ 使得 $[H, \langle g \rangle] = G_3$. 因为 $\langle H, g \rangle$ 正则, 故存在 $a, b \in \langle H, g \rangle$ 使得 $[a, b] = c$ 满足 $\langle a \rangle \bigcap \langle c \rangle = 1$ 且 $G_3 = \langle c \rangle$. 若 $o(a) = p$, 则 $1 = [a^p, b] = c^{pk}$, 其中 $(k, p) = 1$, 从而 $\exp(G_3) \leqslant p$. 若 $o(a) \geqslant p^2$ 且 $o(c) > p$, 则 $[\langle a^p \rangle, \langle H, g \rangle] = \langle c^p \rangle$ 且 $\langle a^p \rangle \ntrianglelefteq G$. 令 $\overline{G} = G/G_3$. 由假设可知, $\overline{G}' \leqslant \langle \bar{a}^p, [\bar{a}^p, \overline{G}] \rangle \leqslant \langle \bar{a}^p \rangle \Phi(\overline{G}')$. 因而 $\overline{G}' = \overline{G}' \bigcap \langle \bar{a}^p \rangle \Phi(\overline{G}') = \overline{G}' \bigcap \langle \bar{a}^p \rangle$. 由此可得 $\langle \bar{a}^p \rangle \trianglelefteq \overline{G}$, 矛盾. 现在设 G_3 不循环. 由假设可知, G_3 的每个循环子群在 G 中正规. 类似于引理 11.6.4(2) 的论证可得, $\exp(G_3) = p$ 且 $G_3 \leqslant Z(G)$.

下证 $|G| \leqslant p^{4w+4}$. 若 G' 的每个循环子群在 G 中正规, 由引理 11.6.4(2) 可得, $\exp(G') = p$ 且 $G' \leqslant Z(G)$. 此时存在 $a, b \in G$ 使得 $a, b \notin \Phi(G)$, $\langle a, b \rangle$ 内交换且

$\langle a\rangle \ntrianglelefteq G$. 因为 $\exp(G')=p$ 且 $d(G)\leqslant w+1$, 故 $G'\leqslant \Omega_1(\langle a\rangle^G)=\Omega_1(\langle a,[\langle a\rangle,G]\rangle)$, 从而 $|G'|\leqslant p^{w+1}$. 令 V 是 G' 的极大子群且 $\widetilde{G}=G/V$. 断言: $|\widetilde{G}|\leqslant p^{2w+2}$. 事实上, 显而易见 $\widetilde{G}$ 有一个内交换子群 $\widetilde{K}$. 若

$$\widetilde{K}=\langle \tilde{a}_1,\tilde{b}_1\mid \tilde{a}_1^{p^m}=\tilde{b}_1^{p^n}=1,\tilde{a}_1^{\tilde{b}_1}=\tilde{a}_1^{1+p^{m-1}}\rangle \quad 且 \quad |\widetilde{G}|=p^{m+n+e},$$

其中 $e\geqslant 0$, 则 $|\widetilde{G}/\langle\tilde{b}_1\rangle^{\widetilde{G}}|=|\widetilde{G}/\langle\tilde{b}_1\rangle\widetilde{G}'|=|\widetilde{G}|/p^{n+1}\leqslant p^w$. 于是 $m\leqslant w+1-e$. 若 $n\leqslant m$, 则 $|\widetilde{G}|\leqslant p^{2w+2}$. 当 $n>m$ 时, 由于 $|\langle\tilde{a}_1\tilde{b}_1^{p^{n-m}}\rangle|=p^m$ 且 $\langle\tilde{a}_1\tilde{b}_1^{p^{n-m}}\rangle\ntrianglelefteq\widetilde{G}$, 故 $n\leqslant w+1-e$. 于是也有 $|\widetilde{G}|\leqslant p^{2w+2}$. 若

$$\widetilde{K}=\langle \tilde{a}_1,\tilde{b}_1,\tilde{c}_1\mid \tilde{a}_1^{p^m}=\tilde{b}_1^{p^n}=\tilde{c}_1^p=1,[\tilde{a}_1,\tilde{b}_1]=\tilde{c}_1,[\tilde{c}_1,\tilde{a}_1]=[\tilde{c}_1,\tilde{b}_1]=1\rangle$$

且 $|G|=p^{m+n+e}$, 其中 $e\geqslant 1$, 则 $m\leqslant w+1-e$ 且 $n\leqslant w+1-e$. 于是 $|\widetilde{G}|\leqslant p^{2w+2}$. 因而 $|G|=|\widetilde{G}||V|\leqslant p^{3w+2}\leqslant p^{4w+4}$. 现在可设存在 $a\in G'$ 使得 $\langle a\rangle\ntrianglelefteq G$. 于是 $G'\leqslant\langle a,[\langle a\rangle,G]\rangle$, 从而 G' 交换. 因为 $d(G)\leqslant w+1$, 故 $d(G')\leqslant w+2$. 于是 $|G_3|\leqslant|\Omega_1(G')|\leqslant p^{w+2}$. 另一方面, 因为 $(G/G_3)'$ 的每个循环子群在 G/G_3 中正规, 由上述论证可知, $|G/G_3|\leqslant p^{3w+2}$. 由此可得 $|G|=|G_3||G/G_3|\leqslant p^{4w+4}$. □

Berkovich[26] 提出了如下问题 (即该文献的问题 148): 研究满足下列条件的有限 p 群 G, 对于每一个非正规子群 H 满足

$$(N_1)\ \exp(H)=\exp(H^G),\quad (N_2)\ |H^G:H|\leqslant p,\quad (N_3)\ H^G=HG'.$$

显然 Dedekind 群满足上述所有的条件. 一般说来, 一个 p 群未必满足上面三个条件中的一个, 吕恒等在文献 [141] 中称满足条件 $(N_i)(i=1,2$ 或 $3)$ 的 p 群 G 为 N_i 群. 该文献研究了 N_3 群, 也研究了同时满足条件 (N_1)—(N_3) 的有限 p 群. 有趣的是, 他们证明了: 由条件 (N_2) 和 (N_3) 可以推出条件 (N_1). 另一方面, 由引理 11.6.3 可知, N_3 群恰为 $\mathcal{C}_a$ 群. 于是以下这两个概念不加区别地使用. 下面介绍 N_3 群的若干结果.

由定理 11.6.5 可看出, 对于 $p\geqslant 3$, $\mathcal{C}_a$ 群 (或者说, N_3 群) 对于幂零类的上界有很强的影响. 然而对于 $p=2$, 结果却不是这样的.

例 11.6.13 设 G 是极大类 2 群. 则 G 是 $\mathcal{C}_a$ 群. 这是因为极大类 2 群 G 一定含有一个指数为 2 的循环群 $\langle c\rangle$. 令 $\langle a\rangle$ 为非正规子群. 则 $a\notin\langle c\rangle$ 且 $G=\langle a,c\rangle$. 由 $G/\langle a\rangle^G$ 循环有 $G'\leqslant\langle a\rangle^G$ 且 $\langle a\rangle^G=\langle a\rangle G'$.

引理 11.6.14 ([141]) 设 G 为 $\mathcal{C}_a$ 群. 则对于任意 $a\in G$ 都有 $\langle a^p\rangle\trianglelefteq G$.

证明 设 $a\in G$ 满足 $\langle a^p\rangle\ntrianglelefteq G$. 则 $\langle a^p\rangle^G=\langle a^p\rangle G'$. 显然 $\langle a\rangle\ntrianglelefteq G$. 令 $H=\langle a\rangle^G=\langle a\rangle G'$. 于是 $|H/\Phi(H)|\geqslant p^2$ 且 $\langle a^p\rangle^G\leqslant\Phi(H)$. 由于 $|\langle a\rangle G':\langle a^p\rangle G'|\leqslant p$, 矛盾. 故 $\langle a^p\rangle\trianglelefteq G$. □

引理 11.6.15 ([141])　设 G 是有限 2 群. 若 G 是 $\mathcal{C}_a$ 群且 $c(G)=2$, 则 G' 不能是阶 $\geqslant 2^2$ 的循环群.

证明　不妨设 G' 是阶为 4 的循环群. 令 $G'=\langle c\rangle$, 其中 $|c|=4$. 由于 $c(G)=2$, 故 G' 是交换群. 于是存在 $a,b\in G$ 满足 $c=[a,b]$. 我们选择 a,b 满足 $c=[a,b]$ 且 $|a|+|b|$ 极小. 因 $[a^2,b]=[a,b^2]=c^2\neq 1$, 故 $a^2\notin\langle a\rangle\bigcap\langle b\rangle$ 且 $b^2\notin\langle a\rangle\bigcap\langle b\rangle$. 由引理 11.6.14 得 $c^2\in\langle a\rangle\bigcap\langle b\rangle$. 于是 $|a|=2^m\geqslant 2^3$ 且 $|b|=2^n\geqslant 2^3$.

(1) 若 $m=n\geqslant 4$, 则由 $a^{2^{m-1}}=b^{2^{m-1}}$ 是 $\langle a\rangle\bigcap\langle b\rangle$ 中的 2 阶元知

$$(ab)^{2^{m-1}}=a^{2^{m-1}}b^{2^{m-1}}c^{2^{m-2}}=a^{2^{m-1}}b^{2^{m-1}}=1.$$

从而 $|ab|\leqslant 2^{m-1}$. 显然 $[a,ab]=[a,b]=c$, 矛盾于 a,b 的选取.

(2) 设 $m\geqslant 4$ 且 $m>n$. 同理可得

$$(a^{2^{m-n}}b)^{2^{n-1}}=a^{2^{m-1}}b^{2^{n-1}}=1,\quad |a^{2^{m-n}}b|\leqslant 2^{2^{n-1}}.$$

由 $[a,a^{2^{m-n}}b]=c$ 可得矛盾.

(3) 若 $m=n=3$, 则 $\langle a\rangle\bigcap\langle b\rangle=\langle a^4\rangle=\langle b^4\rangle=\langle c^2\rangle$. 因 $[a^2c,b]=c^2$ 且 $(a^2c)^2=a^4c^2=1$, 故 $\langle a^2c\rangle\ntrianglelefteq G$. 由 $|a^2c|=2$ 知 $c\notin\langle a^2c\rangle^G$, 矛盾. □

推论 11.6.16 ([141])　设 G 是有限 2 群. 若 G 是 $\mathcal{C}_a$ 群且 $c(G)=2$, 则 G' 是初等交换 2 群.

证明　假设 G' 不是初等交换 2 群. 因 $c(G)=2$, 故 $G'\leqslant Z(G)$, 且存在 $N\trianglelefteq G$ 满足 $N\leqslant G'$ 使得 G'/N 为 4 阶循环群. 考虑 $\overline{G}=G/N$. 则 $\overline{G}$ 是 N_3 群. $\overline{G}'$ 是 4 阶循环群, 矛盾于引理 11.6.15. □

文献 [141] 还得到了其他有趣的结果, 鉴于篇幅所限, 我们不加证明地列出如下.

定理 11.6.17 ([141])　设 G 是 N_3 群. 若 $c(G)\geqslant 3$, 则

(1) 存在 $a,b\in G$ 满足 $G=AB=\langle a,b\rangle B$, 其中 A,B 为 G 的正规子群, $B\bigcap G'$ 为 G' 的真子群且 B 的每个子群都在 G 中正规;

(2) 若 G' 是初等交换群, 则 $\Omega_1(Z(G))\leqslant G'$, 且 (1) 中的子群 B 或者是循环群, 或者 $B\cong \mathrm{Q}_8$, 其中 $p=2$.

定理 11.6.18 ([141])　设 G 既是 N_2 群也是 N_3 群.

(1) 若 $c(G)=2$, 则 $|G'|\leqslant p^2$. 更进一步, 若 $|G'|=p^2$, 则 $p=2$, G' 是初等交换 2 群, 且存在正规子群 N 满足 $\Omega_1(G/N)=(G/N)'$ 为 4 阶初等交换群, 且 $G/N=\overline{G}$ 含有正规子群 $W\cong \mathrm{C}_4\times\mathrm{C}_4$ 和指数最多为 4 的正规亚循环群 $\overline{M}$, 而且 $\overline{G}/\overline{M}$ 是初等交换群.

(2) 若 $c(G)\geqslant 3$, 则 $c(G)=3$ 且下列结论之一成立.

(i) $p=3$ 且

$$G=\langle a,b \mid a^3=b^{-3},[a,b]=c,[c,a]=a^{-3},a^9=b^9=c^3=[c,b]=1\rangle;$$

(ii) $p=2$, $G'\cong C_2\times C_2$ 且

$$G=\langle a,b \mid a^8=b^4=c^2=1,[b,a]=c,[c,a]=b^2,[b,c]=1,a^4=b^2\rangle;$$

(iii) $p=2$, $G'\cong C_4$ 且 $G=H\times E$, 其中 $H=\langle a,b \mid a^8=b^4,a^4=b^2,a^b=a^{-1}\rangle\cong Q_{16}$, 或 $H=\langle a,b \mid a^4=b^8=d^2=1,\ b^a=b^{-1}d,\ [d,a]=[d,b]=1,\ a^2=b^4\rangle$, $E\leqslant Z(G)$ 为初等交换 2 群.

易知定理 11.6.17 和定理 11.6.18 中的群都满足条件 (N_1). 由于满足 $|G'|\leqslant p$ 的 p 群也满足条件 (N_1)—(N_3), 我们可得到下面有趣的结论.

推论 11.6.19 ([141]) 设 G 是有限 p 群. 则由条件 (N_2) 和 (N_3) 可得条件 (N_1).

11.7 非正规子群的正规闭包较小的 p 群

作为 Dedekind 群的另一种推广, 吕恒等在文献 [138], [139] 研究非正规子群的正规闭包较小的有限 p 群. 为便于叙述, 吕恒等称有限 p 群 G 为 $\mathrm{BI}(p^m)$ 群 (或者 $G\in \mathrm{BI}(p^m)$), 若 G 的任意循环子群 H 满足 $|H^G:H|\leqslant p^m$, 其中 m 是正整数. 显然, 任何一个有限 p 群都可看作为某个 $\mathrm{BI}(p^m)$ 群. 另一方面, 有限 Dedekind p 群恰是 $m=0$ 的 $\mathrm{BI}(p^m)$ 群. 文献 [138],[139] 主要研究 $m\leqslant 2$ 的 $\mathrm{BI}(p^m)$ 群及 $m\geqslant 3$ 的某些特殊的 $\mathrm{BI}(p^m)$ 群. 除此之外, 陈贵云、吕恒与他们的同事和学生在 p 群领域还获得了许多其他丰富结果, 见文献 [136], [137], [140]—[143], [249]—[251]. 本节主要介绍他们在文献 [138], [139] 的主要工作.

回顾一下, 群 G 的元素 a 的阶有时用 $o(a)$ 表示, 有时也用 $|a|$ 表示. 本节中用 $|a|$ 表示 a 的阶, $K_i(G)$ 表示幂零群的下中心群列的第 i 项.

11.7.1 $\mathrm{BI}(p)$ 群

Herzog 等在文献 [82] 研究了 J 群的性质. 群 G 称为 J 群 (或者 $G\in J$), 若对于 G 中的每一个元素 x 都有 $\langle x\rangle \lhd G$ 或者对于任意 $g\in G\backslash N_G(\langle x\rangle)$ 都有 $\langle x,x^g\rangle\trianglelefteq G$. 易得 $\mathrm{BI}(p)$ 群一定是 J 群. 但是存在一个 2 群 $G\in J$ 但是 $G\notin \mathrm{BI}(2)$.

例 11.7.1 设群 $G=\langle a,b \mid a^4=1,b^{2^4}=1,a^b=a^3b^{2^2},[a,b^2]=1\rangle$. 则 $|G|=64$, $\langle a\rangle\bigcap\langle b\rangle=1$. 易得 $G\in J$. 但是 $|\langle a\rangle^G:\langle a\rangle|=4$. 因此 $G\notin \mathrm{BI}(2)$.

然而, 对于 $p\geqslant 3$, 有下面结论成立.

命题 11.7.2 设有限 p 群, $p\geqslant 3$. 则 $G\in J$ 当且仅当 $G\in \mathrm{BI}(p)$.

证明　我们仅需要证明: 若 $G \in J$, 则 $G \in \mathrm{BI}(p)$. 假设 $G \in J$ 且存在元 $x \in G$ 使得 $\langle x \rangle$ 不是 G 的正规子群. 则由 [82] 中的引理 7 可知, $\langle x \rangle$ 是 $\langle x \rangle^G = \langle x, x^g \rangle = \langle x, [x,g] \rangle$ 的正规子群, 其中 $g \in G \backslash N_G(\langle x \rangle)$. 又由 [82] 中的定理 13 可知, $[x,g]$ 是 p 阶元. 因此 $|\langle x \rangle^G : \langle x \rangle| \leqslant p$. □

由命题 11.7.2, 仅需研究 BI(2) 群.

引理 11.7.3　设 $G \in \mathrm{BI}(p)$ 且满足 $\exp(G) = p$. 则 $c(G) \leqslant 2$.

证明　由假设可知, 对任意 $a \in G$ 都有 $|\langle a \rangle^G| \leqslant p^2$. 于是 $\langle a \rangle^G \leqslant Z_2(G)$ 且 $a \in Z_2(G)$, 故 $c(G) \leqslant 2$. □

引理 11.7.4　设群 $G = \langle a, b \rangle$ 不是循环群. 若 $|\langle a \rangle^G : \langle a \rangle| \leqslant p, |\langle b \rangle^G : \langle b \rangle| \leqslant p$ 且满足 $\langle a \rangle \bigcap \langle b \rangle = 1$, 则 $c(G) \leqslant 2$ 且 $|G'| \leqslant p$.

证明　由于 $G' \leqslant \langle a \rangle^G \bigcap \langle b \rangle^G$ 且 $|\langle a \rangle^G \bigcap \langle b \rangle^G| \leqslant p^2$, 仅需考虑 $|\langle a \rangle^G \bigcap \langle b \rangle^G| = p^2$. 因此 $|\langle a \rangle \bigcap \langle b \rangle^G| = p$ 且 $|\langle b \rangle \bigcap \langle a \rangle^G| = p$. 若 $|a| = p$, 则 $\langle a \rangle \bigcap \langle b \rangle^G = \langle a \rangle$, 且 $\langle a \rangle \leqslant \langle b \rangle^G$. 因此 $G = \langle b \rangle^G \langle a \rangle = \langle b \rangle^G$. 但是 $\langle b \rangle^G \leqslant \langle b, G' \rangle$ 且 $G = \langle b \rangle$, 与 G 非循环相矛盾. 故 $|a| > p$, $|b| > p$. 令 $\langle a_1 \rangle = \langle a \rangle \bigcap \langle b \rangle^G$ 和 $\langle b_1 \rangle = \langle b \rangle \bigcap \langle a \rangle^G$. 则 $\langle a_1 \rangle, \langle b_1 \rangle$ 分别是 $\langle a \rangle, \langle b \rangle$ 的 p 阶正规子群. 对任意元 $x \in G$, 则 $|\langle a \rangle^G : \langle a \rangle \bigcap \langle a \rangle^x| \leqslant p^2$, 且 $|\langle a \rangle : \langle a \rangle \bigcap \langle a \rangle^x| \leqslant p$. 因此 $\langle a \rangle \bigcap \langle a \rangle^x$ 是 $\langle a \rangle$ 的阶大于或者等于 p 的循环子群. 进而可得 $\langle a_1 \rangle \leqslant \langle a \rangle \bigcap \langle a \rangle^x \leqslant \langle a \rangle^x$. 这说明 $\langle a_1 \rangle \lhd G$ 且 $\langle a_1 \rangle \leqslant Z(G)$. 类似可得 $\langle b_1 \rangle \leqslant Z(G)$.

因为 $\langle a \rangle \bigcap \langle b \rangle = 1$, 所以 $\langle a_1 \rangle \bigcap \langle b_1 \rangle = 1$ 且 $\langle a \rangle^G \bigcap \langle b \rangle^G = \langle a_1, b_1 \rangle$ 是 $Z(G)$ 的一个阶为 p^2 的初等交换群, 即得 $G' \leqslant \langle a \rangle^G \bigcap \langle b \rangle^G \leqslant Z(G)$. 故 $c(G) \leqslant 2$, 且 $G' = \langle [a,b] \rangle$ 是 p 阶循环群. □

引理 11.7.5　设 $G \in \mathrm{BI}(p^k)$. 则对任意 $a \in G$ 有 $|G : N_G(\langle a \rangle)| \leqslant p^k$ 成立.

证明　设 $|a| = p^n$. 因为 G 是 $\mathrm{BI}(p^k)$ 群, 所以 $|\langle a \rangle^G| \leqslant p^{n+k}$. 于是 $\langle a \rangle^G$ 至多存在

$$(p^{n+k} - p^{n-1})/(p^n - p^{n-1}) = p^k + \cdots + 1$$

个阶是 p^n 的循环群. 又对任意 $g \in G$ 有 $\langle a \rangle^g \leqslant \langle a \rangle^G$ 成立, 故 $|G : N_G(\langle a \rangle)| \leqslant p^k$. □

引理 11.7.6　设 $G \in \mathrm{BI}(2)$. 则对任意 $a \in G$ 都满足 $a^{2^{n-1}} \in Z(G)$, 其中 $|a| = 2^n > 2$.

证明　假设元 $b \in G$ 使得 $ab \neq ba$. 令子群 $H = \langle a, b \rangle$. 如果 $\langle a \rangle \bigcap \langle b \rangle \neq 1$, 那么 $a^{2^{n-1}} \in \langle a \rangle \bigcap \langle b \rangle$. 因此 $[a^{2^{n-1}}, b] = 1$. 若 $\langle a \rangle \bigcap \langle b \rangle = 1$, 由引理 11.7.4, 则可得 $c(H) = 2$ 且 $|H'| = 2$. 于是 $[a^{2^{n-1}}, b] = [a,b]^{2^{n-1}} = 1$. 故 $a^{2^{n-1}} \in Z(G)$. □

引理 11.7.7　设 $G = \langle a, b \rangle \in \mathrm{BI}(2)$, 满足 $|a| = 2^n \geqslant 2^4$ 和 $|b| = 2^m \leqslant 2^n$. 若 b 是使得 $G = \langle a, b \rangle$ 的阶最小的元, 则 $\langle a \rangle \bigcap \langle b \rangle = 1$, $c(G) \leqslant 2$ 且 $|G'| \leqslant 2$.

证明 由引理 11.7.4, 仅需要证明 $\langle a\rangle\bigcap\langle b\rangle=1$. 假设 $\langle a\rangle\bigcap\langle b\rangle\neq 1$. 则 $a^{2^{n-1}}=b^{2^{m-1}}$. 下面分三种情况讨论.

(i) $m\leqslant n-2$. 由 [82] 中的推论 15, $a^4\in Z(G)$. 则 $b_1=a^{2^{n-m}}b$ 的阶小于或者等于 2^{m-1}. 显然 $G=\langle a,b_1\rangle$, 与 b 是选择的最小阶元相矛盾.

(ii) $m=n$. 由 [82] 中的命题 10, $c(G)\leqslant 3$. 由 Hall-Petrescu 恒等式,

$$(ab)^{2^{n-1}}=a^{2^{n-1}}b^{2^{n-1}}c_2^{2^{n-1}(2^{n-1}-1)/2}c_3^{2^{n-1}(2^{n-1}-1)(2^{n-1}-2)/6},$$

其中 $c_2\in K_2(G),c_3\in K_3(G)$. 由 [82] 中的命题 12, $\exp(G')\leqslant 4$. 因此 $(ab)^{2^{n-1}}=1$. 从而说明 $|ab|<|b|$. 显然 $G=\langle a,b\rangle=\langle a,ab\rangle$, 再与 b 是选择的最小阶元相矛盾.

(iii) $m=n-1$. 如果 $n\geqslant 5$, 那么 $|a^2b|<|b|$ 且 $G=\langle a,b\rangle=\langle a,a^2b\rangle$. 同理矛盾. 因此我们仅需要考虑 $n=4,m=3$. 由引理 11.7.5 得, $a^2\in N_G(\langle b\rangle)$. 再由 [82] 的推论 15 得, $b^{a^4}=b$. 因此 a^2 诱导出 $\langle b\rangle$ 的一个阶小于或者等于 2 的自同构. 又由 [82] 中的命题 10 得, $\langle a^2,b^2\rangle$ 是交换群. 因此存在整数 k 使得 $b^{a^2}=b^{1+4k}$. 于是可得 $(ba^2)^2=b^{2+4k}a^4$ 且 $(ba^2)^4=b^4a^8=1$. 又 $G=\langle a,b\rangle=\langle a,ba^2\rangle$. 得到矛盾. □

设 $G\in\mathrm{BI}(p)$. 由 [82] 中的命题 10 可知, G 是一个 J 群且 $c(G)\leqslant 3$. 若 $p\geqslant 3$ 且 $c(G)=3$, 由 [82] 中的命题 21 可知, $p=3$ 且 $\exp(G)=3^2$. 对 $p=2$, 我们有如下定理.

定理 11.7.8 *设群 $G\in\mathrm{BI}(2)$. 若 $c(G)=3$, 则 $\exp(G)=4$ 或 8.*

证明 显然仅需要考虑 $\exp(G)\geqslant 4$ 的情形.

假设 $\exp(G)=2^n>8$. 设 $a\in G$ 使得 $|a|=2^n$. 令 $H=\langle a,b\rangle$, 其中 $b\in G$. 又假设 c 是使得 $H=\langle a,c\rangle$ 的阶最小的元. 由引理 11.7.7 得, $\langle a\rangle\bigcap\langle c\rangle=1$ 且 $|H'|\leqslant 2$. 则 $|[a,b]|=|[a,c]|\leqslant 2$.

我们断定 $[a,b]\in Z(G)$. 仅需要考虑 $|[a,b]|=|[a,c]|=2$ 的情形. 若 $|c|=2$, 则 $|\langle c\rangle^G|\leqslant 4$. 由于 $[a,c]\in\langle c\rangle^G$, $[a,c]\in Z(G)$. 设 $|c|\geqslant 4$. 如果 $[a,c]\in\langle a\rangle$ 或者 $[a,c]\in\langle c\rangle$, 由引理 11.7.6 可得, $[a,c]\in Z(G)$. 设 $[a,c]\notin\langle a\rangle$ 且 $[a,c]\notin\langle c\rangle$. 由于 H 也是 BI(2) 群, 由引理 11.7.7 得, $[a,c]\in Z(H)$. 因此 $\langle a\rangle^H=\langle a\rangle\times\langle[a,c]\rangle$ 且 $\langle c\rangle^H=\langle c\rangle\times\langle[a,c]\rangle$. 显然 $\langle a\rangle^G=\langle a\rangle^H$ 且 $\langle c\rangle^G=\langle c\rangle^H$. 于是可得 $H=\langle a\rangle^H\langle c\rangle^H\lhd G$, 且 $\langle[a,c]\rangle=H'\lhd G$. 因为 $|[a,c]|=2$, 所以 $[a,c]\in Z(G)$.

因此若 $|x|=2^n$ 或者 $|y|=2^n$, 则 $[x,y]\in Z(G)$. 不妨设 $|x|,|y|<2^n$. 再次用 Hall-Petrescu 恒等式可得

$$(ax)^{2^{n-1}}=a^{2^{n-1}}x^{2^{n-1}}c_2^{2^{n-1}(2^{n-1}-1)/2}c_3^{2^{n-1}(2^{n-1}-1)(2^{n-1}-2)/6},$$

其中 $c_2\in K_2(\langle a,x\rangle),c_3\in K_3(\langle a,x\rangle)$. 由 [82] 中的命题 12, 则

$$(ax)^{2^{n-1}}=a^{2^{n-1}}x^{2^{n-1}}=a^{2^{n-1}}.$$

这说明 $|ax| = 2^n$. 于是可得 $[ax, y] \in Z(G)$. 因为 $[ax, y] = [a, y]^x[x, y]$, 故 $[x, y] \in Z(G)$. 因此 $G' \leqslant Z(G)$, 与 $c(G) = 3$ 相矛盾. 故 $\exp(G) \leqslant 8$.

若 $\exp(G) = 4$, 类似易得 $\mho_1(G) = G^2 \leqslant Z(G)$. 从而可得 $c(G) \leqslant 2$. 故 $\exp(G) = 8$. □

推论 11.7.9 *设群 G 是非交换的 BI(2) 群. 若 $\exp(G) \geqslant 2^4$, 则 $c(G) = 2$ 且 G' 是初等交换 2 群.*

11.7.2 BI(p^2) 群 ($p\geqslant 3$)

引理 11.7.10 *若群 G 满足 $|G| = p^{m+2}$ 且 $\exp(G) = p^m$, 其中 $m \geqslant 3$, 则 $|G'| \leqslant p^2$.*

证明 由 [26] 中的定理 74.1, G 是亚循环 p 群或 $|\Omega_1(G)| = p^3$ 且 $\exp(\Omega_1(G)) = p$. 若后者成立, 取元 $a \in G$ 使得 $|a| = p^m$, 则 $G = \langle a\rangle\Omega_1(G)$. 因此 $G' \leqslant \Omega_1(G)$, 并且 $|G'| \leqslant p^2$.

设 G 亚循环. 令 R 是阶为 p^2 的正规初等交换群, 并设 $a \in G$ 是 p^m 阶元. 因为 $a^{p^{m-1}}$ 中心化 R, 所以 $|\langle a\rangle \bigcap R| = p$. 又 $(R\langle a\rangle)/R$ 是 G/R 的指数是 p 的循环子群且 G/R 不是循环群. 因此存在元 $b \in G\backslash(R\langle a\rangle)$ 满足 $b^p \in R$, 即 $|b| \leqslant p^2$. 又 $G/(R\langle a^p\rangle)$ 是阶为 p^2 的初等交换群, 故 $R\langle a^p\rangle = \Phi(G)$, 因此 $G = \langle a, b\rangle$. 由于 G 是正则的, $\exp(\langle b\rangle^G) = p^2$, 则由 $G' \leqslant \langle b\rangle^G$ 可得 $\exp(G') \leqslant p^2$. 又 G' 是循环群, 故 $|G'| \leqslant p^2$. □

引理 11.7.11 *设群 $G\in\mathrm{BI}(p^k)$. 则对任意 $a\in G$, $|G : N_G(\langle a\rangle)|\leqslant p^k$ 且 $\langle a^{p^k}\rangle \trianglelefteq G$.*

引理 11.7.12 *设 $G = \langle x, y\rangle \in \mathrm{BI}(p^2)$. 若 $\langle x\rangle \bigcap \langle y\rangle = 1$, 则下列结论成立.*

(1) $c(G) \leqslant 4$. *特别地, 若 $|x| \geqslant |y| \geqslant p^3$, 则 $c(G) \leqslant 3$.*

(2) $|G'| \leqslant p^3$ *且* $\exp(G') \leqslant p^2$.

(3) $\mho_2(G) \leqslant Z(G)$.

证明 设 $|x| = p^m, |y| = p^n$. 由于 $|\langle x\rangle^G : \langle x\rangle| \leqslant p^2$, 则

$$|\langle x\rangle||\langle x^y\rangle|/|\langle x\rangle\bigcap\langle x^y\rangle| = |\langle x\rangle\langle x^y\rangle| \leqslant |\langle x\rangle^G| \leqslant p^{m+2}.$$

从而可得 $|\langle x\rangle \bigcap \langle x^y\rangle| \geqslant p^{m-2}$, 且 $x^{p^2} \in \langle x\rangle \bigcap \langle x^y\rangle$. 因此 $\langle x^{p^2}\rangle = \langle (x^y)^{p^2}\rangle = \langle x^{p^2}\rangle^y$. 令 $H = \langle x^{p^2}, y\rangle$. 则 $\langle x^{p^2}\rangle \lhd H$. 由引理 11.7.11, $x^{p^2} \in N_G(\langle y\rangle)$ 且 $\langle y\rangle \lhd H$. 因为 $\langle x\rangle \bigcap \langle y\rangle = 1$, 所以 $[x^{p^2}, y] = 1$ 且 $x^{p^2} \in Z(G)$. 同理, $y^{p^2} \in Z(G)$.

令 $H = \langle x\rangle^G, K = \langle y\rangle^G$. 则 $G' \leqslant H\bigcap K$. 若 $|H\bigcap K| \leqslant p^3$, 则 $c(G) \leqslant 4$. 若 $|y| \leqslant p^2$, 则 $|K| \leqslant p^4$ 且 $H\bigcap K < K$. 于是也可得 $c(G) \leqslant 4$. 故下面考虑 $|x| \geqslant p^3, |y| \geqslant p^3$ 这种情况. 不妨设 $m \geqslant n \geqslant 3$. 我们将证明 $c(G) \leqslant 3$, 从而证明结论 (1). 由 G 是 BI(p^2) 群且 $\langle x\rangle \bigcap \langle y\rangle = 1$ 可得 $|H \bigcap K| \leqslant p^4$. 若 $|H \bigcap K| = p^3$, 则 $x^{p^{m-1}} \in H \bigcap K$ 且 $y^{p^{n-1}} \in H \bigcap K$. 由于已经得到 $x^{p^{m-1}}, y^{p^{n-1}} \in Z(G)$, 因此

$H\bigcap K \leqslant Z_2(G)$, 这说明 $c(G) \leqslant 3$. 故只考虑 $|H\bigcap K| = p^4$ 这种情况. 此时 $x^{p^{m-2}}, y^{p^{n-2}} \in H\bigcap K$. 又因为 $\langle x\rangle\bigcap\langle y\rangle = 1$, 所以 $H\bigcap K = \langle x^{p^{m-2}}, y^{p^{n-2}}\rangle$. 令 $A = \langle x^{p^{m-1}}, y^{p^{n-1}}\rangle$. 由于对任意 $m,n \geqslant 3$ 都有 $A \leqslant Z(G)$ 成立. 令 $\overline{G} = G/A$. 则 $\overline{G} = \langle\bar{x},\bar{y}\rangle$, 其中 $\bar{x} = xA, \bar{y} = yA$. 于是

$$|\langle\bar{x}\rangle^{\overline{G}} : \langle\bar{x}\rangle| = |HA/A : \langle x\rangle A/A| = |H : \langle x\rangle A| \leqslant p.$$

同理, $|\langle\bar{y}\rangle^{\overline{G}} : \langle\bar{y}\rangle| \leqslant p$. 由引理 11.7.4 可得 $|\overline{G}'| \leqslant p$, 进而 $|G'| \leqslant p^3$. 若 $|G'| \leqslant p^2$, 则 $c(G) \leqslant 3$. 若 $|G'| = p^3$, 则 $A \leqslant G'$. 又 $A \leqslant Z(G)$, 故 $c(G) \leqslant 3$. 即结论 (1) 和 (2) 成立.

设 $g_1 = x^iy^j \in G$. 由 Hall-Petrescu 恒等式可得

$$(x^iy^j)^{p^2} = (x^i)^{p^2}(y^j)^{p^2}a_2^{l_2}a_3^{l_3}a_4^{l_4},$$

其中 $a_i \in K_i(G)$, $l_i = (p^2)!/(p^2-i)!i!$, $i = 2,3,4$. 若 $p \geqslant 5$, 则 $p^2|l_i$. 因为 $\exp(G) \leqslant p^2$, 所以 $g_1^{p^2} = (x^iy^j)^{p^2} = x^{ip^2}y^{jp^2} \in Z(G)$. 又对任何 $g = x^{k_1}y^{m_1}\cdots x^{k_r}y^{m_r} \in G$ 可得

$$g^{p^2} = (x^{k_1})^{p^2}(y^{m_1})^{p^2}\cdots(x^{k_r})^{p^2}(y^{m_r})^{p^2} \in Z(G).$$

假设 $p = 3$. 下证 $\exp(K_3(G)) = 3$.

(i) $|y| = 3$. 则 $K = \langle y\rangle^G$ 的阶小于或者等于 3^3. 因此 K 是正则的且 $\exp(K) = 3$. 又 $G' \leqslant K$, 则 $\exp(G') \leqslant 3$, 即 $\exp(K_3(G)) \leqslant 3$.

(ii) $|x| = |y| = 3^2$. 则 $|H| \leqslant 3^4, |K| \leqslant 3^4$. 因此 $|H\bigcap K| \leqslant 3^3$. 若 $|H\bigcap K| \leqslant 3^2$, 易得 $\exp(K_3(G)) \leqslant 3$. 又设 $|H\bigcap K| = 3^3$. 此时 $|H| = |K| = 3^4$, $|G| = 3^5$ 且 $|G'| \leqslant |H\bigcap K| = 3^3$. 若 $|G'| \leqslant 3^2$, 则 $\exp(K_3(G)) \leqslant 3$. 仅考虑 $|G'| = 3^3$. 若 G' 是循环群, 则 G 是正则的且由 $|x| = |y| = 3^2$ 可得 $\exp(G) = 3^2$, 矛盾. 因此 $|G/\Omega_1(G')| \leqslant 3^3$, 进而 $K_3(G) \leqslant \Omega_1(G')$, 即得 $\exp(K_3(G)) \leqslant 3$.

(iii) $|x| = 3^m \geqslant 3^3$ 且 $|y| = 3^2$. 类似地, 仅考虑 $|H\bigcap K| = 3^3$. 若 $\exp(H\bigcap K) \leqslant 3$, 则 $\exp(K_3(G)) \leqslant 3$. 因此可设 $\exp(H\bigcap K) \geqslant 3^2$. 令 $B = \Omega_1(H\bigcap K)$. 由于 $x^{3^{m-1}}, y^3 \in B$, 则 $|B| = 3^2$. 考虑 $\overline{G} = G/B$. 则 $\overline{G} = \langle\bar{x},\bar{y}\rangle$, 其中 $\bar{x} = xB, \bar{y} = yB$. 由引理 11.7.4 可得 $|\overline{G}'| \leqslant 3$, 即 $K_3(G) \leqslant B$, 进而可得 $\exp(K_3(G)) \leqslant 3$.

(iv) $|x|,|y| \geqslant 3^3$. 由于 $|G'| \leqslant 3^3$ 且 $K_3(G) \leqslant \langle x^{3^{m-1}}\rangle \times \langle y^{3^{n-1}}\rangle$. 因此 $\exp(K_3(G)) \leqslant 3$. 因为 $3^2|l_2, 3^2/l_4$, $3|l_3$ 且 $\exp(K_3(G)) \leqslant 3$, 所以由 Hall-Petrescu 恒等式可得 $\mho_2(G) \leqslant Z(G)$. □

引理 11.7.13 设群 $G = \langle x,y\rangle \in \mathrm{BI}(p^2)$ 是非循环群. 其中 $|x| = p^m$, $|y| = p^n$. 若 $m \geqslant n$ 且 $m \geqslant 3$, 则存在 $y_1 \in G$ 使得 $G = \langle x,y_1\rangle$ 且满足 $\langle x\rangle\bigcap\langle y_1\rangle = 1$, 或者 $\langle x\rangle\bigcap\langle y_1\rangle = \langle y_1^p\rangle$ 且 $|y_1| = p^2$, 其中 $p = 3$.

证明 对 $m+n$ 归纳. 令 $H=\langle x\rangle^G$, $K=\langle y\rangle^G$. 对 m 和 n 的取值分情况讨论.

(a) $n=2$ 且 $\langle x\rangle\bigcap\langle y\rangle=\langle y^p\rangle$.

若 $p=3$, 则 $y_1=y$ 满足条件. 因此可设 $p\geqslant 5$. 令 $M=\langle x^{p^{m-2}},y\rangle$. 此时易得 $|M|\leqslant p^5$ 且 M 是正则的. 由题设可知存在正整数 d 使得 $y^p=x^{dp^{m-1}}$. 进而由 M 的正则性可得 $(yx^{-dp^{m-1}})^p=1$. 令 $y_1=yx^{-dp^{m-1}}$. 则 $G=\langle x,y_1\rangle$ 且 $\langle x\rangle\bigcap\langle y_1\rangle=1$.

(b) $m=n=3$.

下面分两种情况证明 $c(G)\leqslant 5$, $\exp(G')\leqslant p^2$ 且 $\exp(K_3(G))\leqslant p$.

(b1) $\langle x\rangle\bigcap\langle y\rangle=\langle x^p\rangle$: 此时 $x^p\in Z(G)$ 且 $x^p=(x^y)^p$. 因为 G 是 $\mathrm{BI}(p^2)$ 群, 故 $|H|\leqslant p^5$. 由 [26] 中的定理 74.1 得, H 是亚循环群, 或者 $|\Omega_1(H)|=p^3$ 且 $\exp(\Omega_1(H))=p$. 若 H 亚循环, 则 H 是正则群. 因为 $x,x^y\in H$, 故 $(x^{-1}x^y)^p=1$, 且由 $G'\leqslant H$ 可知 $\exp(G')=p$. 因此 $G'\leqslant\Omega_1(H)$. 由 H 亚循环可得 $|\Omega_1(H)|\leqslant p^2$, 进而可得 $c(G)\leqslant 3$. 若 $|\Omega_1(H)|=|\Omega_1(K)|=p^3$ 且 $\exp(\Omega_1(H))=\exp(\Omega_1(K))=p$, 令 $\overline{G}=G/\Omega_1(H)$. 则 $|\bar{x}|=p^2$ 且 $\langle\bar{x}\rangle\lhd\overline{G}$. 显然 $\overline{G}'\leqslant\langle\bar{x}\rangle$. 因此 $|\overline{G}'|\leqslant p$ 且 $K_3(G)\leqslant\Omega_1(H)$. 于是 $\exp(G')\leqslant p^2$, $\exp(K_3(G))\leqslant p$ 且 $c(G)\leqslant 5$.

(b2) $\langle x\rangle\bigcap\langle y\rangle=\langle x^{p^2}\rangle$: 若 $|\Omega_1(H)|=p^3$ 或者 $|\Omega_1(K)|=p^3$, 利用 (b1) 的推论可得 $\exp(G')\leqslant p^2$, $\exp(K_3(G))\leqslant p$ 且 $c(G)\leqslant 5$. 下面再分两种情况讨论.

(b2.1) H,K 都是亚循环群且 $H\bigcap K$ 是循环群: 因为 $G'\leqslant H\bigcap K$, 故 $G'=\langle[x,y]\rangle$. 又 $x,x^y\in H$ 且 $x^{p^2}=(x^{p^2})^y=(x^y)^{p^2}$, 由 H 正则可得 $[x,y]^{p^2}=1$. 于是 $|G'|\leqslant p^2$ 且 $|K_3(G)|\leqslant p$, $c(G)\leqslant 3$.

(b2.2) H,K 都是亚循环群且 $H\bigcap K$ 是非循环群: 由于 $p\geqslant 3$, $|\Omega_1(H\bigcap K)|\geqslant p^2$, 则 $|\Omega_1(H)|=|\Omega_1(K)|=p^2$. 因此 $\Omega_1(H)=\Omega_1(H\bigcap K)=\Omega_1(K)$. 令 $\overline{G}=G/\Omega_1(H)$. 则 $\overline{G}=\langle\bar{x},\bar{y}\rangle$, $\langle\bar{x}\rangle\bigcap\langle\bar{y}\rangle=1$ 且 $|\langle\bar{x}\rangle^{\overline{G}}:\langle\bar{x}\rangle|\leqslant p, |\langle\bar{y}\rangle^{\overline{G}}:\langle\bar{y}\rangle|\leqslant p$. 故由引理 11.7.4 可得 $|\overline{G}'|\leqslant p$, 且 $K_3(G)\leqslant\Omega_1(H)$. 因此 $\exp(G')\leqslant p^2$, $\exp(K_3(G))\leqslant p$, 且 $c(G)\leqslant 4$.

又由于 $\langle x\rangle\bigcap\langle y\rangle=\langle y^p\rangle$ 或 $\langle y^{p^2}\rangle$, 故 $x^{p^2}=y^{kp^2}$, 其中 $1\leqslant k\leqslant p-1$. 因为 $c(G)\leqslant 5$, 由 Hall-Petrescu 恒等式可得

$$(xy^{-k})^{p^2}=x^{p^2}y^{-kp^2}c_2^{n_2}c_3^{n_3}c_4^{n_4}c_5^{n_5},$$

其中 $c_i\in K_i(G)$ 且 $p^2|n_2,p|n_3,p|n_4,p|n_5$. 于是 $(xy^{-k})^{p^2}=1$. 令 $y_0=xy^{-k}$, 则 $G=\langle x,y_0\rangle$ 且 $|y_0|\leqslant p^2$. 由 (a), 则存在元 y_1 使得 $G=\langle x,y_1\rangle$ 且 $\langle x\rangle\bigcap\langle y_1\rangle=1$, 或 $\langle x\rangle\bigcap\langle y_1\rangle=\langle y_1^3\rangle$ 且 $|y_1|=9$.

(c) $m=n\geqslant 4$.

下面分两种情况讨论.

(c1) $\langle x^{p^2}\rangle \leqslant \langle x\rangle\bigcap\langle y\rangle$: 此时 $x^{p^2}\in Z(G)$ 且 $\langle x^{p^3}\rangle \lhd G$. 令 $\overline{G}=G/\langle x^{p^3}\rangle=\langle\bar{x},\bar{y}\rangle$. 易得 $|\bar{x}|=|\bar{y}|=p^3$. 又由 (b) 可知, 存在 $y_1\in G$ 使得 $\overline{G}=\langle\bar{x},\bar{y}_1\rangle$ 且 $|\bar{y}_1|\leqslant p^2$. 于是 $G=\langle x,y_1\rangle$ 且 $|y_1|<|x|$. 令 $G_0=\langle x^p,y_1\rangle$. 由归纳法可知, 存在 y_2 使得 $G_0=\langle x^p,y_2\rangle$ 且 $\langle x^p\rangle\bigcap\langle y_2\rangle=1$ 或 $\langle y_2^p\rangle$. 此时 $p=3$. 因此 $G=\langle x,G_0\rangle=\langle x,y_2\rangle$ 且 $\langle x\rangle\bigcap\langle y_2\rangle=1$ 或 $\langle y_2^p\rangle$ 且 $|y_2|=9$.

(c2) $\langle x\rangle\bigcap\langle y\rangle=\langle x^{p^{m-1}}\rangle$: 下证 $\exp(G')\leqslant p^3$, $\exp(K_3(G))\leqslant p^2$, $\exp(K_4(G))\leqslant p$ 且 $c(G)\leqslant 6$. 由 [26] 中的定理 74.1, H 是亚循环群或者 $|\Omega_1(H)|=p^3$ 且 $\exp(\Omega_1(H))=p$. 同理 K 是亚循环群或者 $|\Omega_1(K)|=p^3$ 且 $\exp(\Omega_1(K))=p$. 下面再分三种情形讨论.

(c2.1) 若 $|\Omega_1(H)|=p^3$ 且 $\exp(\Omega_1(H))=p$: 令 $\overline{G}=G/\Omega_1(H)=\langle\bar{x},\bar{y}\rangle$. 显然 $\langle\bar{x}\rangle\bigcap\langle\bar{y}\rangle=1$. 由引理 11.7.12 可知 $\exp(\overline{G}')\leqslant p^2$. 因为 $|\bar{x}|=p^{m-1}=|\overline{H}|$, 所以 $\langle\bar{x}\rangle=\overline{H}\lhd\overline{G}$. 于是 $\overline{G}'$ 是阶不超过 p^2 的循环群. 因此可得 $\exp(G')\leqslant p^3$, $\exp(K_3(G))\leqslant p^2$ 且 $\exp(K_4(G))\leqslant p$. 又因为 $|G'|\leqslant p^5$, 所以 $c(G)\leqslant 6$.

(c2.2) H,K 是亚循环群且 $H\bigcap K$ 是循环群: 因为 $G'\leqslant H\bigcap K$, 所以 G' 是循环群, 由此可得 $G'=\langle[x,y]\rangle$. 令 $\overline{G}=G/\langle x^{p^{m-1}}\rangle=\langle\bar{x},\bar{y}\rangle$. 则 $\langle\bar{x}\rangle\bigcap\langle\bar{y}\rangle=1$. 由引理 11.7.12 可得 $|[\bar{x},\bar{y}]|\leqslant p^2$ 且 $|[x,y]|\leqslant p^3$. 因此 $\exp(G')\leqslant p^3$, $\exp(K_3(G))\leqslant p^2$, $\exp(K_4(G))\leqslant p$ 且 $c(G)\leqslant 4$.

(c2.3) H,K 是亚循环群且 $H\bigcap K$ 是非循环群: 由 (b2.2), 可得 $\Omega_1(H)=\Omega_1(K)$ 的阶是 p^2. 令 $\overline{G}=G/\Omega_1(H)=\langle\bar{x},\bar{y}\rangle$. 易得 $|\langle\bar{x}\rangle^{\overline{G}}:\langle\bar{x}\rangle|\leqslant p$, $|\langle\bar{y}\rangle^{\overline{G}}:\langle\bar{y}\rangle|\leqslant p$ 且 $\langle\bar{x}\rangle\bigcap\langle\bar{y}\rangle=1$. 又由引理 11.7.4 可知 $|\overline{G}'|\leqslant p$. 因此 $|G'|\leqslant p^3$. 此时也得 $\exp(G')\leqslant p^3$, $\exp(K_3(G))\leqslant p^2$, $\exp(K_4(G))\leqslant p$ 且 $c(G)\leqslant 4$. 由于存在正整数 $l\leqslant p-1$ 使得 $\langle x\rangle\bigcap\langle y\rangle=\langle x^{p^{m-1}}\rangle$, $x^{p^{m-1}}=y^{-lp^{m-1}}$. 由 Hall-Petrescu 恒等式又得

$$(xy^l)^{p^{m-1}}=x^{p^{m-1}}y^{lp^{m-1}}c_2^{n_2}c_3^{n_3}c_4^{n_4}c_5^{n_5}c_6^{n_6},$$

其中, $c_i\in K_i(G)$, $n_i=(p^{m-1})!/(p^{m-1}-i)!i!$, $i=2,3,\cdots,6$. 因为 $p\geqslant 3$, 所以当 $i=3,\cdots,6$ 时, $p^3|n_2,p^2|n_i$. 于是 $(xy^l)^{p^{m-1}}=1$. 由此可得 $G=\langle x,xy^l\rangle$ 且 $|x|>|xy^l|$. 由归纳法知, 存在 $y_1\in G$ 使得 $G=\langle x,y_1\rangle$ 且 $\langle x\rangle\bigcap\langle y_1\rangle=1$ 或 $\langle y_1^3\rangle$ 且 $|y_1|=9$.

(c3) $\langle x\rangle\bigcap\langle y\rangle=\langle x^{p^{m-k}}\rangle$: 此时 $k\geqslant 2$. 令 $\overline{G}=G/\langle x^{p^{m-k-1}}\rangle=\langle\bar{x},\bar{y}\rangle$. 由 (c2) 可得元 $y_0\in G$ 使得 $\overline{G}=\langle\bar{x},\bar{y}_0\rangle$ 并且满足 $|\bar{y}_0|<|\bar{y}|$. 因此 $G=\langle x,y_0\rangle$ 满足 $|y_0|<|y|$. 由归纳法存在元 y_1 满足要求.

(d) $m>n\geqslant 3$.

令 $G_1=\langle x^{p^{m-n}},y\rangle$. 由归纳法存在 y_1 使得 $G_1=\langle x^{p^{m-n}},y_1\rangle$ 且 $\langle x^{p^{m-n}}\rangle\bigcap\langle y_1\rangle=1$ 或 $\langle y_1^3\rangle$ 且 $|y_1|=9$. 故 $G=\langle x,G_1\rangle=\langle x,y_1\rangle$ 满足条件. □

定理 11.7.14 设 $G\in \mathrm{BI}(p^2)$. 则 $\mho_2(G)\leqslant Z(G)$ 且 $\exp(G')\leqslant p^2$.

证明　首先 $\mho_2(G) \leqslant Z(G)$. 取 $x \in G$ 使得 $|x| = p^m \geqslant p^3$. 对任意 $y \in G$, 令 $G_1 = \langle x, y\rangle$. 仅需证明 $[x^{p^2}, y] = 1$. 若 $\langle x\rangle \bigcap \langle y\rangle = 1$, 由引理 11.7.12 可得, $\mho_2(G_1) \leqslant Z(G_1)$, 于是 $[x^{p^2}, y] = [x, y^{p^2}] = 1$.

(i) $|y| \leqslant p^2$. 由前面讨论, 下面考虑 $|y| = p^2$ 且 $\langle x\rangle \bigcap \langle y\rangle = \langle y^p\rangle$ 的情形. 若 $m = 3$, 则 $x^{p^2} \in \langle y^p\rangle \leqslant Z(G_1)$. 因此 $[x^{p^2}, y] = 1$. 设 $m > 3$ 且 $x_0 \in \langle x\rangle$ 使得 $x_0^p = y^{-p}$. 再由引理 11.7.5 可得 $|\langle x\rangle : N_{\langle x\rangle}(\langle y\rangle)| \leqslant p^2$, 进而 $\langle x_0\rangle$ 正规化 $\langle y\rangle$. 因此 $[x_0, y] \in \langle y^p\rangle$, 即 $\langle x_0, y\rangle$ 的阶是 p^3 且幂零类不超过 2. 令 $y_1 = x_0 y$ 使得 $y_1^p = x_0^p y^p = 1$ 且 $G_1 = \langle x, y\rangle = \langle x, y_1\rangle$. 由引理 11.7.12 可得, $x^{p^2} \in Z(G_1)$.

(ii) $|y| \geqslant p^3$. 不妨设 $|x| \geqslant |y|$. 若存在 y_1 使得 $G_1 = \langle x, y\rangle = \langle x, y_1\rangle$ 且 $\langle x\rangle \bigcap \langle y_1\rangle = 1$, 则由引理 11.7.12 可得 $\mho_2(G_1) \leqslant Z(G_1)$. 这表明 $[x^{p^2}, y] = [x, y^{p^2}] = 1$. 再由引理 11.7.13 可知, 存在特殊情况 $p = 3$, $G_1 = \langle x, y\rangle = \langle x, y_1\rangle$, $\langle x\rangle \bigcap \langle y_1\rangle = \langle y_1^3\rangle$ 且 $|y_1| = 9$. 由 (i) 可得 $G_1 = \langle x, y_1\rangle$, 于是 $x^{3^2} \in Z(G_1)$.

下面证明 $\exp(G') \leqslant p^2$.

断定对任意 $x, y \in G$ 有 $|[x, y]| \leqslant p^2$. 若 $|y| \leqslant p^2$, 则 $|\langle y\rangle^G| \leqslant p^4$. 假设 $\exp(\langle y\rangle^G) \geqslant p^3$. 若 $\exp(\langle y\rangle^G) = p^4$, 则 $\langle y\rangle^G$ 是 G 的循环子群, 即 $\langle y\rangle \lhd G$, 矛盾. 因此 $\exp(\langle y\rangle^G) = p^3$. 于是存在 $w \in \langle y\rangle^G$ 使得 $|w| = p^3$. 进而说明 $\langle y\rangle^G$ 是正则群, 即 $\exp(\langle y\rangle^G) = |y| \leqslant p^2$, 矛盾. 因此 $\exp(\langle y\rangle^G) \leqslant p^2$, 即对任意 $x \in G$ 和任意 $[x, y] \in \langle y\rangle^G$ 有 $|[x, y]| \leqslant p^2$. 若 $|x| \geqslant |y| \geqslant p^3$, 令 $G_1 = \langle x, y\rangle$. 由引理 11.7.13 可知, 存在 $y_1 \in G$ 使得 $G_1 = \langle x, y\rangle = \langle x, y_1\rangle$ 且 $\langle x\rangle \bigcap \langle y_1\rangle = 1$ 或 $\langle y_1^3\rangle$ 且 $|y_1| = 9$. 若 $\langle x\rangle \bigcap \langle y_1\rangle = 1$, 由引理 11.7.12 可得 $|[x, y]| \leqslant p^2$. 若 $\langle x\rangle \bigcap \langle y_1\rangle \neq 1$, 则 $|y_1| = 3^2$. 类似地, $|[x, y]| \leqslant 3^2$.

对任意 $a, b \in G$ 且满足 $|a|, |b| \leqslant p^2$, 下面证明 $\exp(\langle a, b\rangle) \leqslant p^2$. 令 $A = \langle a, b\rangle$, $H = \langle a\rangle^A, K = \langle b\rangle^A$. 因此 $|H|, |K| \leqslant p^4$ 且 $|A| \leqslant p^6$. 若 $|A| = p^6$, 易得 $|H \bigcap K| \leqslant p^2$. 于是 $|A'| \leqslant p^2$, $|K_3(A)| \leqslant p$ 且 $c(A) \leqslant 3$. 由 Hall-Petrescu 恒等式可得 $\exp(A) \leqslant p^2$. 不妨设 $|A| \leqslant p^5$. 若 $\exp(A) \geqslant p^3$, 由 [26] 中的定理 74.1 可得, A 亚循环或 $|\Omega_1(A)| = p^3$ 且 $\exp(\Omega_1(A)) = p$. 若 A 亚循环, 则 A 是正则的. 于是 $\exp(A) \leqslant p^2$. 若 $|\Omega_1(A)| = p^3$ 且 $\exp(\Omega_1(A)) = p$. 则 $\exp(\Omega_2(A)) \leqslant p^2$. 但是 $a, b \in \Omega_2(A)$, 矛盾. 因此 $\exp(A) \leqslant p^2$, 从而可得 $\exp(G') \leqslant p^2$. □

定理 11.7.15　*设群* $G \in \mathrm{BI}(p^2)$. *则* $c(G) \leqslant 4$.

证明　显然仅需证明: 对任意 $x, y \in G$ 均有 $[x, y] \in Z_3(G)$. 设

$$|x| = p^m, \quad |y| = p^n, \quad H = \langle x\rangle^G, \quad K = \langle y\rangle^G.$$

若 $|H \bigcap K| \leqslant p^3$, 则由 $[x, y] \in H \bigcap K$ 可得 $[x, y] \in Z_3(G)$.

(i) 设 $m \leqslant 2$ 且 $n \leqslant 2$. 则 $|H|, |K| \leqslant p^4$ 且 $|H'|, |K'| \leqslant p^2$. 若 $y \in H$, 则 $[x, y] \in H'$, 于是 $[x, y] \in Z_2(G) \leqslant Z_3(G)$. 类似地, 若 $x \in K$. 则 $[x, y] \in Z_3(G)$. 又

设 $x \notin K$, $y \notin H$. 则 $|H\bigcap K| \leqslant p^3$, 从而也得 $[x,y] \in Z_3(G)$.

(ii) 设 $m \leqslant 2$ 且 $n \geqslant 3$. 因为 $|H| \leqslant p^4$, 只需要考虑 $|H\bigcap K| = p^4$ 这种情况, 即 $H \leqslant K$. 由引理 11.7.10 可得 $|K'| \leqslant p^2$. 因此也可得 $[x,y] \in Z_3(G)$. 对于 $m \geqslant 3$ 且 $n \leqslant 2$, 结论同样成立.

(iii) 设 $m \geqslant 3$ 且 $n \geqslant 3$. 若 $\langle x\rangle \bigcap \langle y\rangle = 1$, 则 $|H\bigcap K| \leqslant p^4$. 类似地仅需假设 $|H\bigcap K| = p^4$. 因此 $x^{p^{m-1}} \in \langle x\rangle \bigcap K$ 且 $x^{p^{m-1}} \in H\bigcap K$. 同理 $y^{p^{n-1}} \in H\bigcap K$. 由定理 11.7.14 可得 $x^{p^{m-1}}, y^{p^{n-1}} \in Z(G)$. 进而 $H\bigcap K \leqslant Z_3(G)$ 且 $[x,y] \in Z_3(G)$. 若 $\langle x\rangle \bigcap \langle y\rangle \neq 1$. 令 $G_1 = \langle x, y\rangle$. 不妨设 $m \geqslant n$. 由引理 11.7.13 可知, 存在元 y_1 使得 $G_1 = \langle x, y\rangle = \langle x, y_1\rangle$ 且 $\langle x\rangle \bigcap \langle y_1\rangle = 1$ 或 $\langle y_1^3\rangle$ 且 $|y_1| = 9$. 若 $\langle x\rangle \bigcap \langle y_1\rangle = 1$, 同上可得 $G_1' \leqslant Z_3(G)$, 进而有 $[x,y] \in Z_3(G)$. 此时 $\langle x\rangle \bigcap \langle y_1\rangle \neq 1$, 由 (ii), 因为 $|y_1| = 9$, 所以也有 $[x,y] \in G_1' \leqslant Z_3(G)$. □

引理 11.7.16 *设群 $G \in \mathrm{BI}(p^2)$. 若存在元 $x, y \in G$ 使得 $\langle x\rangle \bigcap \langle y\rangle = 1$, 其中 $|x| = p^m \geqslant p^3$, $|y| = p^n \geqslant p^3$, 则 $[x,y] \in Z_2(G)$.*

证明 由定理 11.7.14 可知 $x^{p^{m-1}}$, $y^{p^{n-1}} \in Z(G)$. 令 $H = \langle x\rangle^G, K = \langle y\rangle^G$. 因为 G 是 $\mathrm{BI}(p^2)$ 群, 故 $|H\bigcap K| \leqslant p^4$. 若 $|H\bigcap K| \leqslant p^2$, 则 $[x,y] \in H\bigcap K \leqslant Z_2(G)$. 若 $|H\bigcap K| = p^3$, 则 $x^{p^{m-1}}$, $y^{p^{n-1}} \in Z(G)$ 且 $[x,y] \in H\bigcap K \leqslant Z_2(G)$. 因此设 $|H\bigcap K| = p^4$. 若 $m \geqslant 4$, 则由定理 11.7.14 可知 $x^{p^{m-2}} \in Z(G)$. 因为 $y^{p^{n-1}} \in Z(G)$ 且 $x^{p^{m-2}}$, $y^{p^{n-1}} \in H\bigcap K$, 故 $[x,y] \in H\bigcap K \leqslant Z_2(G)$. 类似可证, 当 $n \geqslant 4$ 时结论也成立.

设 $|H\bigcap K| = p^4$ 且 $m = n = 3$. 因为 $\langle x\rangle \bigcap \langle y\rangle = 1$, 故 $|H\bigcap \langle y\rangle| = p^2$. 于是 $y^p \in H$. 因此 $H = \langle x, y^p\rangle = \langle x\rangle\langle y^p\rangle$ 的阶是 p^5. 又由 $HK = H\langle y\rangle$ 可知 $HK \lhd G$ 的阶是 p^6. 但是由于 $|\langle x\rangle\langle y\rangle| = |\langle x\rangle||\langle y\rangle| = p^6$, 于是 $HK = \langle x\rangle\langle y\rangle$. 又由 [89] 中的III, 定理 11.5 可知, HK 是亚循环群. 从而可得 $\exp(HK) = p^3$. 这表明 $(HK)' \lhd G$ 是阶不超过 p^2 的循环群. 故 $[x,y] \in (HK)' \leqslant Z_2(G)$. □

定理 11.7.17 *设群 $G \in \mathrm{BI}(p^2)$. 则 $c(G) \leqslant 3$ 当且仅当 $[\Omega_2(G), G] \leqslant Z_2(G)$.*

证明 仅需证明充分性. 取元 $x, y \in G$. 若 $|y| \leqslant p^2$(或者 $|x| \leqslant p^2$), 则由题设 $[x,y] \in Z_2(G)$. 因此假设 $|x| \geqslant |y| \geqslant p^3$. 令子群 $G_1 = \langle x, y\rangle$. 由引理 11.7.13, 存在元 y_1 使得 $G_1 = \langle x, y_1\rangle$ 且 $\langle x\rangle \bigcap \langle y_1\rangle = 1$, 或者 $\langle x\rangle \bigcap \langle y_1\rangle = \langle y_1^3\rangle$ 且 $|y_1| = 9$. 若 $|y_1| \leqslant p^2$, 由题设 $[x, y_1] \in Z_2(G)$, 即 $[x,y] \in G_1' \leqslant Z_2(G)$. 若 $|y_1| \geqslant p^3$, 则 $\langle x\rangle \bigcap \langle y_1\rangle = 1$. 由引理 11.7.16, $[x, y_1] \in Z_2(G)$, 即 $[x,y] \in G_1' \leqslant Z_2(G)$. 故 $c(G) \leqslant 3$. □

定理 11.7.18 *设群 $G \in \mathrm{BI}(p^2)$. 若 $c(G) = 4$, 则 $\mho_2(G)$ 循环.*

证明 假设 $\mho_2(G)$ 不循环. 仅需由 $\exp(G) = p^m \geqslant p^3$ 推出矛盾即可.

取 $x \in G$ 使得 $|x| = p^m = \exp(G)$. 我们将证明对任意 $y \in G$ 满足 $[x,y] \in Z_2(G)$. 令 $G_1 = \langle x, y\rangle$. 由引理 11.7.13 可知, 存在 $y_1 \in G_1$ 使得$G_1 = \langle x, y_1\rangle$ 且

$\langle x\rangle\bigcap\langle y_1\rangle=1$ 或 $\langle y_1^3\rangle$ 且$|y_1|=3^2$. 若 $|y_1|\geqslant p^3$, 则 $\langle x\rangle\bigcap\langle y_1\rangle=1$. 又由引理 11.7.16 可得 $[x,y_1]\in Z_2(G)$. 于是 $[x,y]\in Z_2(G)$. 不妨设 $|y_1|\leqslant p^2$. 此时包含情况 $p=3$, $\langle x\rangle\bigcap\langle y_1\rangle=\langle y_1^3\rangle$ 且 $|y_1|=3^2$. 断言: 存在元 $z\in G$ 使得 $z^{p^2}\notin\langle x\rangle$. 若否, 对任意 $g\in G$ 有 $g^{p^2}\in\langle x\rangle$. 因为 $|x|=p^m=\exp(G)$, 故 $g^{p^2}\in\langle x^{p^2}\rangle$, 即 $\mho_2(G)=\langle x^{p^2}\rangle$ 是循环群, 矛盾. 令 $G_2=\langle x,z\rangle$. 由引理 11.7.13 知, 存在 $z_1\in G_2$ 使得 $G_2=\langle x,z_1\rangle$ 且 $\langle x\rangle\bigcap\langle z_1\rangle=1$ 或 $\langle z_1^3\rangle$ 且 $|z_1|=3^2$. 若 $|z_1|\leqslant p^2$, 则由 G_2' 是 $\langle z_1\rangle^{G_2}$ 的真子群且 $G_2\in\mathrm{BI}(p^2)$ 可得 $|G_2'|\leqslant p^3$. 又由定理 11.7.14 得 $\exp(G_2')\leqslant p^2$. 若 $|G_2'|=p^3$, 则 $|\Omega_1(G_2')|\geqslant p^2$, 即 $K_3(G_2)\leqslant\Omega_1(G_2')$. 因此 $\exp(K_3(G_2))\leqslant p$. 由 Hall-Petrescu 恒等式可得 $(xz_1)^{p^2}=x^{p^2}z_1^{p^2}=x^{p^2}$. 于是对任意 $g_2\in G_2$ 都有 $g_2^{p^2}\in\langle x^{p^2}\rangle$ 成立, 这与 z 的选择相矛盾. 因此 $|z_1|\geqslant p^3$, 即 $\langle x\rangle\bigcap\langle z_1\rangle=1$. 又由引理 11.7.16 可得 $[x,z_1]\in Z_2(G)$. 令 $a=z_1y_1$. 因为 $|y_1|\leqslant p^2$, 同上类似可得 $|z_1|\leqslant p^2$. 于是 $a^{p^2}=z_1^{p^2}y_1^{p^2}=z_1^{p^2}$. 由此可得 $|a|=|z_1|$ 且 $\langle x\rangle\bigcap\langle a\rangle=1$. 由引理 11.7.16 可得 $[x,a]\in Z_2(G)$. 因为 $[x,a]=[x,z_1][x,y_1]^{z_1}$, 故 $[x,y_1]^{z_1}=[x,z_1]^{-1}[x,a]\in Z_2(G)$, 即 $[x,y]\in Z_2(G)$.

下面将证明: 对任意 $x_1,x_2\in G$ 都有 $[x_1,x_2]\in Z_2(G)$, 从而得到与题设 $c(G)=4$ 相矛盾. 若 $|x_1|=p^m$ 或 $|x_2|=p^m$, 则 $[x_1,x_2]\in Z_2(G)$. 因此可设 $|x_1|<p^m$ 且 $|x_2|<p^m$. 令 $G_3=\langle x,x_1\rangle$. 由引理 11.7.13 知, 存在 $x_1'\in G_3$ 使得 $G_3=\langle x,x_1'\rangle$ 且 $\langle x\rangle\bigcap\langle x_1'\rangle=1$ 或 $\langle x_1'^3\rangle$ 满足 $|x_1'|=9$. 若 $\langle x\rangle\bigcap\langle x_1'\rangle=1$, 由引理 11.7.12 得 $|G_3'|\leqslant p^3$. 若 $|x_1'|=3^2$, 由前面的讨论可知 $|G_3'|\leqslant 3^3$. 因此 $K_3(G_3)\leqslant\Omega_1(G_3')$. 再由 Hall-Petrescu 恒等式可得

$$(xx_1)^{p^{m-1}}=x^{p^{m-1}}x_1^{p^{m-1}}=x^{p^{m-1}},$$

即 $|xx_1|=p^m$. 于是可得 $[xx_1,x_2]\in Z_2(G)$. 由于 $[x,x_2]\in Z_2(G)$, 故 $[x_1,x_2]\in Z_2(G)$, 矛盾. □

11.7.3 BI(2^2) 群

引理 11.7.19 设 $G=\langle a,b\rangle\in\mathrm{BI}(2^2)$. 若 $\langle a\rangle\bigcap\langle b\rangle=1$, 则下列结论成立.

(1) $\mho_2(G)\leqslant Z(G)$;

(2) $|G'|\leqslant 2^3$ 且 $\exp(G')\leqslant 2^2$.

证明 设 $|a|=2^m,|b|=2^n$. 由引理 11.7.5 可得 $\langle a^4\rangle\trianglelefteq G$ 且 $\langle b\rangle^{a^4}=\langle b\rangle$. 又 $\langle a\rangle\bigcap\langle b\rangle=1$, 于是 $[a^4,b]=1$, 即 $a^4\in Z(G)$. 同理 $b^4\in Z(G)$.

下面证明 (2) 成立. 分如下两种情况讨论.

(i) $n\leqslant 2$. 此时 $|\langle b\rangle^G|\leqslant 2^4$ 且 $|G'|\leqslant 2^3$. 下证 $\exp(G')\leqslant 2^2$. 设 $|G'|=2^3$. 若 $\langle a\rangle\bigcap G'=1$, 由于 $G'\leqslant\langle a\rangle^G$, 则 $2^2\geqslant|\langle a\rangle^G:\langle a\rangle|\geqslant|\langle a\rangle G':\langle a\rangle|=2^3$, 矛盾. 因此 $\langle a\rangle\bigcap G'\neq 1$, 即 $a^{2^{m-1}}\in G'$. 同理, $b^2\in G'$, 这说明对任意 $\langle a\rangle\bigcap\langle b\rangle=1$ 都有

$\exp(G')\leqslant 2^2$. 对 $m\leqslant 2$ 类似可证.

(ii) $m\geqslant n\geqslant 3$. 则 $|\langle a\rangle^G\bigcap\langle b\rangle^G|\leqslant 2^4$. 由于 $G'\leqslant\langle a\rangle^G\bigcap\langle b\rangle^G$, 仅需考虑 $2^3\leqslant|\langle a\rangle^G\bigcap\langle b\rangle^G|\leqslant 2^4$ 的情形. 因此 $a^{2^{m-1}}\in\langle a\rangle^G\bigcap\langle b\rangle^G$ 且 $b^{2^{n-1}}\in\langle a\rangle^G\bigcap\langle b\rangle^G$. 令 $N=\langle a^{2^{m-1}},b^{2^{n-1}}\rangle$. 显然 $N\leqslant Z(G)$. 令 $\overline{G}=G/N$. 则 $|\langle\bar{a}\rangle^{\overline{G}}:\langle\bar{a}\rangle|\leqslant 2$ 且 $|\langle\bar{b}\rangle^{\overline{G}}:\langle\bar{b}\rangle|\leqslant 2$. 由引理 11.7.4, $|\overline{G}'|\leqslant 2$, 即可得 $|G'|\leqslant 2^3$ 且 $\exp(G')\leqslant 2^2$.

由 $|G'|\leqslant 2^3$ 且 $\exp(G')\leqslant 2^2$ 可知 $|\mho_1(G')|\leqslant 2$. 因此对任意 $x\in G'$ 有 $x^2\in Z(G)$. 设 $g_1=a^ib^j\in G$. 由 Hall-Petrescu 恒等式可得

$$(a^ib^j)^4=(a^i)^4(b^j)^4c_2^{\binom{4}{2}}c_3^{\binom{4}{3}}c_4^{\binom{4}{4}},$$

其中 $c_i\in K_i(G)$, $i=2,3,4$. 由于 $c_2^{\binom{4}{2}}=(c_2^2)^3\in Z(G)$, $c_3^{\binom{4}{3}}=c_3^4=1\in Z(G)$, $c_4^{\binom{4}{4}}=c_4\in Z(G)$. 因此 $g_1^4\in Z(G)$. 于是对任意 $g=a^{k_1}b^{l_1}\cdots a^{k_r}b^{l_r}\in G$, 对 r 归纳可得 $g^4\in Z(G)$. □

引理 11.7.20 设群 $G\in\mathrm{BI}(2^2)$. 则对任意 $a\in G$ 满足 $|\langle a^2\rangle^G:\langle a^2\rangle|\leqslant 2$.

证明 不妨设 $|a|\geqslant 4$. 由引理 11.7.5 可知, $\langle a^4\rangle\trianglelefteq G$. 设 $\overline{G}=G/\langle a^4\rangle$. 则 $|\bar{a}|=4$ 且 $|\langle\bar{a}\rangle^{\overline{G}}|\leqslant 2^4$. 设 $\overline{K}=\langle\bar{a}\rangle^{\overline{G}}$. 若 $|\overline{K}|\leqslant 2^2$, 则 $\overline{K}=\langle\bar{a}\rangle$, 即 $\langle a\rangle\trianglelefteq G$. 设 $|\overline{K}|\geqslant 2^3$. 则 $\overline{K}$ 是非循环. 从而可得 $|\overline{K}:\Phi(\overline{K})|\geqslant 2^2$, 这说明 $|\mho_1(\overline{K})|\leqslant 4$. 显然, $\langle\bar{a}^2\rangle^{\overline{G}}\leqslant\mho_1(\overline{K})$. 因此 $|\langle\bar{a}^2\rangle^{\overline{G}}:\langle\bar{a}^2\rangle|\leqslant 2$, 进而得到 $|\langle a^2\rangle^G:\langle a^2\rangle|\leqslant 2$. □

引理 11.7.21 设 $G=\langle a,b\rangle$ 是非循环 2 群且满足 $\langle a\rangle\bigcap\langle b\rangle\neq 1$, $|a|=|b|=2^4$, $|\langle a\rangle^G:\langle a\rangle|\leqslant 2$. 若 $|\langle b\rangle^G:\langle b\rangle|\leqslant 2$, 或 $|\langle b\rangle^G:\langle b\rangle|\leqslant 4$ 且 $\langle a^{2^2}\rangle\leqslant\langle a\rangle\bigcap\langle b\rangle$, 则 $|ab|\leqslant 2^3$.

证明 设 $c=[a,b]$. 因为 $|\langle a\rangle^G:\langle a\rangle|\leqslant 2$ 且 $c\in\langle a\rangle^G$, 故 $c^2\in\langle a\rangle$, 即 $(c^2)^a=c^2$. 又 G 非循环, 故 $\langle a\rangle\neq\langle b\rangle$. 下面分三种情况讨论.

(1) $|\langle a\rangle\bigcap\langle b\rangle|=2^3$. 此时 $\langle a^2\rangle=\langle b^2\rangle=\langle a\rangle\bigcap\langle b\rangle\leqslant Z(G)$. 因为 $|\langle a\rangle^G:\langle a\rangle|\leqslant 2$, 故 $|G/\langle a^2\rangle|\leqslant 2^3$, 即可得 $|(G/\langle a^2\rangle)'|\leqslant 2$. 又 $a^2\in Z(G)$, 则 G' 是交换群. 由于 $1=[a^2,b]=[a,b]^a[a,b]$, 则 $c^a=c^{-1}$, 即 $(c^2)^a=c^{-2}$. 我们已经证明了 $(c^2)^a=c^2$, 故 $|c|\leqslant 2^2$. 由 G' 交换可得 $\exp(G')\leqslant 4$. 因为 $|(G/\langle a^2\rangle)'|\leqslant 2$, 故 $K_3(G)\leqslant\langle a^2\rangle\leqslant Z(G)$, 即 $c(G)\leqslant 3$.

(2) $|\langle a\rangle\bigcap\langle b\rangle|=2^2$. 则 $\langle a^{2^2}\rangle=\langle b^{2^2}\rangle=\langle a\rangle\bigcap\langle b\rangle\leqslant Z(G)$. 同上可得 $|G/\langle a^{2^2}\rangle|\leqslant 2^5$. 由题设 $2^4\leqslant|\langle a\rangle^G|\leqslant 2^5$.

若 $|\langle a\rangle^G|=2^4$, 则 $\langle a\rangle^G=\langle a\rangle$, 即 $a^b=a^k$, 其中 $(k,2)=1$. 因为 $\langle a^{2^2}\rangle=\langle a\rangle\bigcap\langle b\rangle\leqslant Z(G)$, 故 $a^4=(a^4)^b=a^{4k}$. 于是 $k=1+4k_1$. 因此 $c=[a,b]=a^{4k_1}$, 即 $c^4=1$. 此时可得 $G'=\langle c\rangle$, 其阶小于 2^2. 故 $c(G)\leqslant 3$ 且 $\exp(G')\leqslant 4$.

又设 $|\langle a\rangle^G|=2^5$. 显然 $\langle a\rangle^G$ 非循环. 若 $c\in\langle a\rangle$, 则 $a^b\in\langle a\rangle$ 且 $\langle a\rangle=\langle a\rangle^G$, 矛盾. 因此 $\langle a\rangle^G=\langle a,c\rangle$. 因为 $a^4\in\langle a\rangle^G\bigcap Z(G)$, 由定理 1.9.1 得, $\langle a\rangle^G\cong \mathrm{C}_{2^4}\times\mathrm{C}_2$ 或

$\langle a\rangle^G \cong \mathrm{M}_2(4,1)$. 设 $\langle a\rangle^G = \langle a,d\rangle$, 其中 $d^2=1, a^d=d$ 或 a^{1+8}. 又设 $a^b=a^ld$, 其中 $(2,l)=1$. 则 $(a^2)^b=a^lda^ld$. 若 $a^d=a$, 则 $(a^2)^b=a^{2l}$ 且 $(a^4)^b=a^{4l}$. 若 $a^d=a^{1+8}$, 则 $(a^2)^b=a^lda^ld=a^{10l}$ 且 $(a^4)^b=a^{20l}=a^{4l}$. 因此 $l=1+4l_1$, l_1 是整数. 即可得 $[a,b]=c=a^{4l_1}d$, 由 $[a^{4l_1},d]=1$ 可得 $c^4=a^{2^4l_1}=1$. 易得 $|\Omega_2(\langle a\rangle^G)|\leqslant 2^3$ 且 $\exp(\Omega_2(\langle a\rangle^G))\leqslant 4$. 因为 $|c|\leqslant 4$, 故 $G'=\langle c^g|g\in G\rangle\leqslant\Omega_2(\langle a\rangle^G)$. 由此得 $|G'|\leqslant 2^3$, $\exp(G')\leqslant 4$ 且 $c(G)\leqslant 4$.

(3) $|\langle a\rangle\bigcap\langle b\rangle|=2$. 此时 $\langle a^{2^3}\rangle=\langle a\rangle\bigcap\langle b\rangle\leqslant Z(G)$. 设 $\overline{G}=G/\langle a^{2^3}\rangle$. 则 $\langle\bar a\rangle\bigcap\langle\bar b\rangle=1$. 由题设可得 $|\langle a\rangle^G:\langle a\rangle|\leqslant 2$ 且 $|\langle b\rangle^G:\langle b\rangle|\leqslant 2$. 因此 $|\langle\bar a\rangle^{\overline{G}}:\langle\bar a\rangle|\leqslant 2$, $|\langle\bar b\rangle^{\overline{G}}:\langle\bar b\rangle|\leqslant 2$. 由引理 11.7.4 可知, $|\overline{G}'|\leqslant 2$, 进而可得 $|G'|\leqslant 4$ 且 $c(G)\leqslant 3$.

综上 $\exp(G')\leqslant 4$ 且 $c(G)\leqslant 4$. 由 Hall-Petrescu 恒等式可得

$$(ab)^{2^3}=a^{2^3}b^{2^3}c_2^{\binom{8}{2}}c_3^{\binom{8}{3}}c_4^{\binom{8}{4}},$$

其中 $c_i\in K_i(G), i=2,3,4$. 因此 $|a|=2^4$ 且 $a^{2^3}=b^{2^3}$. 于是 $(ab)^{2^3}=1$. □

引理 11.7.22　*设 $G=\langle a,b\rangle\in\mathrm{BI}(2^2)$, 其中 $|a|=2^5, |b|\leqslant 2^4$. 若 $\langle a\rangle\bigcap\langle b\rangle\neq 1$, 则存在元 $b_1\in G$ 使得 $G=\langle a,b_1\rangle$, 并满足 $\langle a\rangle\bigcap\langle b_1\rangle=1$ 和 $|b_1|<|b|$.*

证明　设 $|b|=2^4$. 令 $H=\langle a^2,b\rangle$. 由引理 11.7.20 可得 $|\langle a^2\rangle^H:\langle a^2\rangle|\leqslant 2$. 若 $|\langle a^2\rangle\bigcap\langle b\rangle|\geqslant 4$, 由引理 11.7.21 可得 $|a^2b|\leqslant 2^3$. 设 $h=a^2b$. 则 $|h|\leqslant 2^3$ 且 $G=\langle a,h\rangle$.

下面首先假设 $|\langle a^2\rangle\bigcap\langle b\rangle|=2$. 则 $\langle b^{2^3}\rangle=\langle a^2\rangle\bigcap\langle b\rangle\leqslant Z(G)$. 设 $\overline{H}=H/\langle b^8\rangle$. 又设 $\overline{A}=\langle\bar a^2\rangle^{\overline{H}}\bigcap\langle\bar b\rangle^{\overline{H}}$. 则 $|\overline{A}|\leqslant|\langle\bar b\rangle^{\overline{H}}|\leqslant 2^5$. 若 $|\overline{A}|\geqslant 2^4$, 则 $|\langle\bar b\rangle^{\overline{H}}:\overline{A}|\leqslant 2$. 由此可得 $\bar b^2\in\overline{A}$. 于是 $\bar b^2\in\langle\bar a^2\rangle^{\overline{H}}$. 然而

$$|\langle a^2\rangle^H:\langle a^2\rangle|=|\langle\bar a^2\rangle^{\overline{H}}:\langle\bar a^2\rangle|\geqslant|\langle\bar a^2\rangle\langle\bar b^2\rangle:\langle\bar a^2\rangle|=|\langle\bar b^2\rangle|=4.$$

这与 $|\langle a^2\rangle^H:\langle a^2\rangle|\leqslant 2$ 相矛盾. 因此 $|\overline{A}|\leqslant 2^3$.

若 $|\overline{A}|=2^3$. 因为 $|\overline{A}:\langle\bar a^2\rangle\bigcap\langle\bar b\rangle^{\overline{H}}|\leqslant|\langle\bar a^2\rangle^{\overline{H}}:\langle\bar a^2\rangle|=|\langle a^2\rangle^H:\langle a^2\rangle|\leqslant 2$, 故 $|\langle\bar a^2\rangle\bigcap\langle\bar b\rangle^{\overline{H}}|\geqslant 2^2$, 这表明 $\bar a^4\in\overline{A}$. 又 $|\langle\bar a\rangle^{\overline{H}}:\langle\bar a\rangle|\leqslant 4$, 故 $|\overline{A}\bigcap\langle\bar b\rangle|=2$, 于是 $\bar b^4\in\overline{A}$. 从而可得 $\overline{A}=\langle\bar a^4,\bar b^4\rangle$. 由于 $\overline{H}'\leqslant\overline{A}$, 则 $\overline{H}'\leqslant\langle\bar a^4,\bar b^4\rangle$ 且 $H'\leqslant\langle a^4,b^4\rangle$. 断言 $|H'|\leqslant 2^3$. 若否, 则由 $|\langle a^4,b^4\rangle|=2^4$ 可得 $H'=\langle a^4,b^4\rangle$. 由引理 11.7.5 可得 $\langle a^4\rangle\trianglelefteq G$ 且 $\langle b^4\rangle\trianglelefteq G$. 再由定理 1.9.1, 则 $H'\cong\mathrm{M}_2(3,1)$ 或 $H'\cong\mathrm{C}_8\times\mathrm{C}_2$. 设 $c=[a^2,b]$. 则 $c^2\in\langle a^4\rangle$. 由引理 11.7.5 得 a^4 正规化 $\langle b\rangle$, 即 $\langle\bar b\rangle\trianglelefteq\overline{H}$. 由 $\langle\bar a^4\rangle\trianglelefteq\overline{H}$ 可得 $[\bar a^4,\bar b]=\bar 1$. 于是 $[a^2,b]^{a^2}[a^2,b]=c^{a^2}c\in\langle b^8\rangle$. 设 $|c|=2^3$. 因为 $H'\cong\mathrm{M}_2(3,1)$ 或 $\mathrm{C}_8\times\mathrm{C}_2$, 故 $\mho_2(H')=\langle b^8\rangle$, 由此即得 $c^4=b^8$. 进而可得 $c^{a^2}=c^{-1}c^4$ 或 $c^{a^2}=c^{-1}$. 从而有 $(c^2)^{a^2}=c^{-2}$. 但是 $c^2\in\langle a^4\rangle$. 故 $c^4=1$, 矛盾. 因此 $|c|\leqslant 4$. 显然 $\exp(\Omega_2(H'))\leqslant 4$ 且 $|\Omega_2(H')|\leqslant 2^3$, 矛盾. 于是证得 $|H'|\leqslant 2^3$.

若 $\exp(H')=2^3$, 则 $H'=\langle c\rangle$ 循环. 设 $\langle a^2\rangle\bigcap\langle c\rangle=1$. 则 $|\bar{c}|=|c|=2^3$. 因此 $\overline{A}=\langle\bar{c}\rangle$. 因为 $|\overline{A}:\langle\bar{a}^2\rangle\bigcap\langle\bar{b}\rangle^{\overline{H}}|\leqslant 2$, 故 $|\langle\bar{a}^2\rangle\bigcap\langle\bar{b}\rangle^{\overline{H}}|\geqslant 2$, 即 $\bar{a}^8\in\overline{A}=\langle\bar{c}\rangle$. 于是 $\bar{a}^8=\bar{c}^4$. 由此可得 $c^4\in\langle a^2\rangle$, 矛盾. 因此 $\langle a^2\rangle\bigcap\langle c\rangle\neq 1$, 即 $c^4\in\langle a^2\rangle$ 且 $c^4=a^{16}=b^8$. 由引理 11.7.5 得 $c^{a^2}=c^{-1}c^4$ 或 $c^{a^2}=c^{-1}$. 这说明 $c^2\notin\langle a^2\rangle$. 因而 $\langle c\rangle\bigcap\langle a^2\rangle=\langle b^8\rangle=\langle a^{2^4}\rangle$, 即 $\langle\bar{c}\rangle\bigcap\langle\bar{a}^2\rangle=1$. 但是 $\bar{c}\in\langle\bar{a}^2\rangle^{\overline{H}}$, 由此可得 $|\langle\bar{a}^2\rangle^{\overline{H}}:\langle\bar{a}^2\rangle|=4$, 矛盾. 故 $\exp(H')\leqslant 4$ 且 $|H'|\leqslant 2^3$. 由 Hall-Petrescu 恒等式得

$$(a^2b)^8=(a^2)^{2^3}b^8c_2^{\binom{8}{2}}c_3^{\binom{8}{3}}c_4^{\binom{8}{4}}=a^{2^4}b^{2^3}=1,$$

其中 $c_i\in K_i(H), i=2,3,4$. 设 $h=a^2b$. 则 $G=\langle a,h\rangle$ 且 $|h|\leqslant 2^3$.

由于 $|\overline{A}|\leqslant 2^2$, 易得 $|H'|\leqslant 2^3$. 同上, 则可找到 b_1 使得 $G=\langle a,b_1\rangle$ 满足 $\langle a\rangle\bigcap\langle b_1\rangle=1$ 且 $|b_1|<|b|$.

最后假设 $|h|=2^3$. 令 $H_1=\langle a^4,h\rangle$. 由引理 11.7.5 可知, $\langle a^4\rangle\trianglelefteq H_1$ 且 $\langle h\rangle\trianglelefteq H_1$. 因此 $c(H_1)\leqslant 2$. 若 $\langle a^4\rangle\bigcap\langle h\rangle=\langle h^2\rangle$, 则 $[a^4,h]^2=[a^4,h^2]=1$, 即 $(a^4h)^4=1$. 若 $\langle a^4\rangle\bigcap\langle h\rangle=\langle h^4\rangle$, 则 $|H_1'|\leqslant 2$, 也可得 $(a^4h)^4=a^{2^4}h^4=1$. 设 $x=a^4h$. 则 $H_1=\langle a^4,x\rangle$ 且元 $|x|\leqslant 4$. 显然 $G=\langle a,H\rangle=\langle a,H_1\rangle=\langle a,x\rangle$. 设 $\langle a\rangle\bigcap\langle x\rangle=\langle x^2\rangle$. 考虑子群 $K=\langle a^4,x\rangle$. 设 $\langle a^4\rangle\bigcap\langle x\rangle\neq 1$. 由引理 11.7.5 得 $\langle a^4\rangle\trianglelefteq K$ 且 $\langle x\rangle\trianglelefteq K$. 因此 $K\cong \mathrm{M}_2(3,1)$ 或 $\mathrm{C}_8\times\mathrm{C}_2$. 由此可得 $[a^8,x]=1$. 此时存在 b_1 使得 $\langle a^8,x\rangle=\langle a^8\rangle\times\langle b_1\rangle$ 且 $b_1^2=1$. 因此 $G=\langle a,x\rangle=\langle a,b_1\rangle$. 显然 $\langle a\rangle\bigcap\langle b_1\rangle=1$ 且 $|b_1|<|b|$. 对于 $|h|\leqslant 2^2$, 类似可证得相同的结论.

若 $|b|=2^2$. 同上可以找到 $b_1\in\langle a^4,b\rangle$ 使得 $\langle a^4,b\rangle=\langle a^4,b_1\rangle$ 满足 $\langle a^4\rangle\bigcap\langle b_1\rangle=1$ 且 $|b_1|<|b|$. 因此 $G=\langle a,b_1\rangle$, 其中 $\langle a\rangle\bigcap\langle b_1\rangle=1$ 且 $|b_1|<|b|$. □

引理 11.7.23 *设 $G=\langle a,b\rangle\in \mathrm{BI}(2^2)$, 其中 $|a|=2^m$, $|b|=2^n$ 且 $m\geqslant 5$, $m\geqslant n$. 若 $\langle a\rangle\bigcap\langle b\rangle\neq 1$, 则存在元 $b_1\in G$ 使得 $G=\langle a,b_1\rangle$ 且满足 $\langle a\rangle\bigcap\langle b_1\rangle=1$ 和 $|b_1|<|b|$.*

证明 首先设 $m=5$. 由引理 11.7.22, 仅需考虑 $|b|=2^5$. 分两种情形讨论.

情形 1 存在子群 $N\leqslant G'$ 使得 $N\cong \mathrm{C}_2\times\mathrm{C}_2$ 且 $N\trianglelefteq G$.

再分两种情形讨论.

(i) $\langle a^{16}\rangle\leqslant N$.

设 $\overline{G}=G/N=\langle\bar{a},\bar{b}\rangle$. 因为 $N\leqslant G'\leqslant\langle a\rangle^G\bigcap\langle b\rangle^G$, 故 $\langle\bar{a}\rangle^{\overline{G}}=\langle a\rangle^GN/N=\langle a\rangle^G/N$. 于是 $|\langle\bar{a}\rangle^{\overline{G}}:\langle\bar{a}\rangle|=|\langle a\rangle^G/N:\langle a\rangle N/N|\leqslant 2$. 同理 $|\langle\bar{b}\rangle^{\overline{G}}:\langle\bar{b}\rangle|\leqslant 2$. 显然, $|\bar{a}|=|\bar{b}|=2^4$. 若 $\langle\bar{a}\rangle\bigcap\langle\bar{b}\rangle=1$, 由引理 11.7.4 得 $|\overline{G}'|\leqslant 2$, 即 $|G'|\leqslant 2^3$. 因此 $c(G)\leqslant 4$. 由 Hall-Petrescu 恒等式得

$$(ab)^{2^4}=(a)^{2^4}(b)^{2^4}c_2^{\binom{16}{2}}c_3^{\binom{16}{3}}c_4^{\binom{16}{4}},$$

其中 $c_i \in K_i(G)$. 因而 $(ab)^{2^4}=1$. 又 $G=\langle a, ab\rangle$, 由引理 11.7.22 知, 存在 $b_1\in G$ 使得 $G=\langle a,b_1\rangle$ 且 $\langle a\rangle\bigcap\langle b_1\rangle=1$. 若 $\langle\bar{a}\rangle\bigcap\langle\bar{b}\rangle\neq 1$, 由引理 11.7.21 知, 存在 $x\in G$ 使得 $\overline{G}=\langle\bar{a},\bar{x}\rangle$ 且 $|\bar{x}|\leqslant 2^3$. 又由 $N\leqslant G'$ 可得 $G=\langle a,x,N\rangle=\langle a,x\rangle$. 显然 $|x|\leqslant 2^4$. 由引理 11.7.22 知, 存在 b_1 使得 $G=\langle a,b_1\rangle$ 满足 $\langle a\rangle\bigcap\langle b_1\rangle=1$ 和 $|b_1|<|b|$.

(ii) $\langle a^{16}\rangle\not\leqslant N$.

设 $N_1=N\langle a^{16}\rangle$. 由 $\langle a^{16}\rangle\leqslant Z(G)$ 可知 $N_1\cong \mathrm{C}_2\times\mathrm{C}_2\times\mathrm{C}_2$. 设 $\overline{G}=G/N_1$. 若 $\langle\bar{a}\rangle\bigcap\langle\bar{b}\rangle\neq 1$, 证明与 (i) 类似可得. 若 $\langle\bar{a}\rangle\bigcap\langle\bar{b}\rangle=1$, 由引理 11.7.4 可得 $|\overline{G}'|\leqslant 2$, 即 $|G'|\leqslant 2^4$. 因此 $c(G)\leqslant 5$. 由 N_1 是初等交换群可知 $\exp(G')\leqslant 2^2$. 再由 Hall-Petrescu 恒等式得

$$(ab)^{2^4}=(a)^{2^4}(b)^{2^4}c_2^{\binom{16}{2}}c_3^{\binom{16}{3}}c_4^{\binom{16}{4}}c_5^{\binom{16}{5}},$$

其中 $c_i\in K_i(G)$. 因此 $|ab|\leqslant 2^4$. 类似 (i), 也存在 $b_1\in G$ 使得 $G=\langle a,b_1\rangle$ 满足 $\langle a\rangle\bigcap\langle b_1\rangle=1$ 且 $|b_1|<|b|$.

情形 2 不存在子群 $K\leqslant G'$ 使得 $K\trianglelefteq G$ 且 $K\cong\mathrm{C}_2\times\mathrm{C}_2$.

由推论 1.9.2 得, G' 循环或同构于 $\mathrm{D}_{2^r},\mathrm{Q}_{2^r},\mathrm{SD}_{2^r}$. 令 $c=[a,b]$. 下面分四种情形证明: $\exp(G')\leqslant 2^3$ 且 $\exp(K_4(G))\leqslant 2^2$.

(1) $|\langle a\rangle\bigcap\langle b\rangle|=2^4$: 此时 $\langle a\rangle\bigcap\langle b\rangle=\langle a^2\rangle\leqslant Z(G)$. 设 $\overline{G}=G/\langle a^2\rangle$. 因为 $\overline{G}\in\mathrm{BI}(2^2)$, 故 $|\overline{G}|\leqslant 2^4$, 即 $|\overline{G}'|\leqslant 2^2$. 因此由 $a^2\in Z(G)$ 可得 $c(G)\leqslant 4$.

若 $\overline{G}'$ 循环, 则 G' 交换. 从而可得 $G'=\langle c\rangle$ 循环. 因为 $a^2\in Z(G)$, 故 $1=[a^2,b]=[a,b]^a[a,b]$, 即 $c^a=c^{-1}$. 但是 $c^4\in\langle a^2\rangle$, 因而 $c^4=(c^4)^a=c^{-4}$, 即 $|c|\leqslant 2^3$. 于是 $|G'|=|\langle c\rangle|\leqslant 2^3$ 且 $\exp(G')\leqslant 2^3$, $\exp(K_3(G))\leqslant 2^2$, $\exp(K_4(G))\leqslant 2$.

若 $\overline{G}'\cong\mathrm{C}_2\times\mathrm{C}_2$, 则 $G'\cong\mathrm{D}_{2^r},\mathrm{Q}_{2^r}$ 或 SD_{2^r}. 因为 $\overline{G}'=G'\langle a^2\rangle/\langle a^2\rangle$ 且 $a^2\in Z(G)$, 故 $c(G')\leqslant 2$. 从而 $|G'|\leqslant 2^3$. 于是 $\exp(G')\leqslant 2^2$, 且 $\exp(K_4(G))\leqslant 2^2$.

(2) $|\langle a\rangle\bigcap\langle b\rangle|=2^3$: 此时 $\langle a\rangle\bigcap\langle b\rangle=\langle a^4\rangle\leqslant Z(G)$. 设 $\overline{G}=G/\langle a^4\rangle$. 因为 $\overline{G}\in\mathrm{BI}(2^2)$, 故 $|\overline{G}|\leqslant 2^6$. 再分两种情形讨论.

(2.1) $|\overline{G}|=2^6$: 此时 $|\langle\bar{a}\rangle^{\overline{G}}\bigcap\langle\bar{b}\rangle^{\overline{G}}|=4$. 因此 $\overline{G}'$ 循环或 $\overline{G}'\cong\mathrm{C}_2\times\mathrm{C}_2$. 若 $\overline{G}'\cong\mathrm{C}_2\times\mathrm{C}_2$, 则由 (1) 可得 $\exp(G')\leqslant 2^3$, $c(G)\leqslant 4$ 且 $\exp(K_4(G))\leqslant 2^2$. 若 $\overline{G}'$ 循环, 则由 $\langle a^4\rangle\leqslant Z(G)$ 可知 G' 交换. 因而 $G'=\langle c\rangle$. 设 $|c|=2^l$. 显然 $c^4\in\langle a^4\rangle\leqslant Z(G)$ 且 $l\leqslant 5$. 设 $c^a=c^k$, 其中 $(2,k)=1$ 且 $k\leqslant 2^l$. 因为

$$1=[a^4,b]=[a,b]^{a^3}[a,b]^{a^2}[a,b]^a[a,b],$$

故 $c^{k^3}c^{k^2}c^kc=1$. 又 $c^4\in Z(G)$, 故 $c^4=(c^4)^a=c^{4k}$. 于是

$$\begin{cases} k^3+k^2+k+1\equiv 0(\bmod\ 2^l),\\ 4k\equiv 4(\bmod\ 2^l).\end{cases}\tag{11.1}$$

若 $l=4$ 或者 $l=5$, 则方程组没有解. 因而 $l\leqslant 3$. 由此可得 $|c|\leqslant 2^3$. 则 $|G'|=|\langle c\rangle|\leqslant 2^3$, 即 $c(G)\leqslant 4$, $\exp(G')\leqslant 2^3$, $\exp(K_4(G))\leqslant 2$.

(2.2) $|\overline{G}|\leqslant 2^5$: 若 $\langle\bar{a}\rangle\bigcap\langle\bar{b}\rangle=1$, 由定理 1.9.1 可得 $\overline{G}$ 不是极大类群. 因此 $|\overline{G}'|\leqslant 2^2$. 于是 $\overline{G}'\cong \mathrm{C}_2\times\mathrm{C}_2$ 或 $\overline{G}'$ 循环. 类似 (2.1) 可得 $\exp(G')\leqslant 2^3$, $c(G)\leqslant 4$ 且 $\exp(K_4(G))\leqslant 2^2$.

(3) $|\langle a\rangle\bigcap\langle b\rangle|=2^2$: 此时 $\langle a\rangle\bigcap\langle b\rangle=\langle a^8\rangle\leqslant Z(G)$. 设 $\overline{G}=G/\langle a^8\rangle$. 由引理 11.7.19 得 $|\overline{G}'|\leqslant 2^3$, 即 $|G'|\leqslant 2^5$. 再分两种情形讨论.

(3.1) $|\overline{G}'|=2^3$: 因为 $4\geqslant|\langle\bar{a}\rangle^{\overline{G}}:\langle\bar{a}\rangle|=|\langle\bar{a}\rangle\overline{G}':\langle\bar{a}\rangle|=|\overline{G}':\langle\bar{a}\rangle\bigcap\overline{G}'|$, 故 $|\langle\bar{a}\rangle\bigcap\overline{G}'|\geqslant 2$, 即 $\bar{a}^4\in\overline{G}'$. 同理 $\bar{b}^4\in\overline{G}'$. 由 $\overline{G}'$ 不循环可知 G' 不循环. 若 $|G'|=2^5$, 则 $a^8\leqslant G'$. 因为 $a^8\in Z(G)$, 故 G' 不是极大类群. 由推论 1.9.2 知, G' 存在 G 的正规子群 $\mathrm{C}_2\times\mathrm{C}_2$, 与假设矛盾. 因此 $|G'|\leqslant 2^4$. 又 G' 非循环. 显然 $\exp(G')\leqslant 2^3$. 因为 $c(\overline{G})\leqslant 3$, 故 $K_4(G)\leqslant\langle a^8\rangle$, 于是 $c(G)\leqslant 4$ 且 $\exp(K_4(G))\leqslant 2^2$. 若 $|G'|\leqslant 2^3$, 则由 G' 可得 $\exp(G')\leqslant 2^2$. 故 $c(G)\leqslant 4$.

(3.2) 设 $|\overline{G}'|\leqslant 2^2$: 若 $\overline{G}'\cong\mathrm{C}_2\times\mathrm{C}_2$, 类似 (2.1) 可得 $\exp(G')\leqslant 2^3$, $K_4(G)\leqslant\langle a^8\rangle$ 且 $c(G)\leqslant 4$. 若 $\overline{G}'$ 循环, 则 G' 交换且 $G'=\langle c\rangle$. 显然 $|G'|\leqslant 2^4$. 设 G' 是阶为 2^4 的循环群, 则 $\langle a^8\rangle=\langle c^4\rangle$. 不妨设 $c^a=c^l$, 其中 $(2,l)=1$ 且 $l\leqslant 2^4$. 因为 $(c^4)^a=c^4$, 故 $c^{4l}=c^4$. 因此 $l=1,9$ 或 13. 又 $\langle a^8\rangle=\langle b^8\rangle$ 且 $c^{a^4}=c$, 故

$$1=[a^8,b]=[a^4,b]^{a^4}[a^4,b]=[a^4,b]^2.$$

于是 $([a,b]^{a^3}[a,b]^{a^2}[a,b]^a[a,b])^2=1$. 因此 $c^{2(l^3+l^2+l+1)}=1$. 易得 $l\neq 1,9,13$. 从而可得 $|c|\leqslant 2^3$. 故 $\exp(G')\leqslant 2^3$, $c(G)\leqslant 4$ 且 $\exp(K_4(G))\leqslant 2^2$.

(4) $|\langle a\rangle\bigcap\langle b\rangle|=2$: 此时 $\langle a\rangle\bigcap\langle b\rangle=\langle a^{2^4}\rangle\leqslant Z(G)$, 易得 $|\overline{G}'|\leqslant 2^3$ 且 $\exp(\overline{G}')\leqslant 2^2$. 因此可得 $\exp(G')\leqslant 2^3$, $c(G)\leqslant 4$ 且 $\exp(K_4(G))\leqslant 2^2$. 由 Hall-Petrescu 恒等式得

$$(ab)^{2^4}=(a)^{2^4}(b)^{2^4}c_2^{\binom{16}{2}}c_3^{\binom{16}{3}}c_4^{\binom{16}{4}},$$

其中 $c_i\in K_i(G)$. 从而有 $(ab)^{2^4}=(a)^{2^4}(b)^{2^4}=1$. 于是 $G=\langle a,ab\rangle$ 且 $|ab|\leqslant 2^4$. 由引理 11.7.22, 存在 $b_1\in G$ 使得 $G=\langle a,b_1\rangle$ 满足 $\langle a\rangle\bigcap\langle b_1\rangle=1$ 且 $|b_1|<|b|$.

对 $m\geqslant 6$, 我们对 $m+n$ 归纳. 设 $\langle a\rangle\bigcap\langle b\rangle=\langle a^{2^{m-k}}\rangle$, 其中 $k\geqslant 1$. 若 $k\leqslant 4$, 令 $\overline{G}=G/\langle a^{2^{m-5}}\rangle=\langle\bar{a},\bar{b}\rangle$. 则 $|\bar{a}|=2^5$ 且 $|\bar{b}|\leqslant 2^5$. 由引理 11.7.22 知, 存在 $b_0\in G$ 使得 $\overline{G}=\langle\bar{a},\bar{b_0}\rangle$ 满足 $\langle\bar{a}\rangle\bigcap\langle\bar{b}_0\rangle=1$ 和 $|\bar{b}_0|<|\bar{b}|$. 则 $G=\langle a,b_0\rangle$ 且 $|b_0|\leqslant 2^{n-1}$. 由归纳法, 存在 $b_1\in G$ 使得 $G=\langle a,b_1\rangle$ 满足 $\langle a\rangle\bigcap\langle b_1\rangle=1$ 和 $|b_1|<|b|$. 若 $k\geqslant 5$, 令 $\tilde{G}=G/\langle a^{2^{m-k-1}}\rangle$. 由归纳法, 存在 b_2 使得 $\tilde{G}=\langle\tilde{a},\tilde{b}_2\rangle$ 且 $\langle\tilde{a}\rangle\bigcap\langle\tilde{b}_2\rangle=1$. 从而可得 $G=\langle a,b_2\rangle$ 且 $|b_2|<|b|$. 因此, 再由归纳法, 存在 $b_1\in G$ 使得 $G=\langle a,b_1\rangle$ 且 $\langle a\rangle\bigcap\langle b_1\rangle=1$, $|b_1|<|b|$. □

由引理 11.7.19 可知, 对于 $G=\langle a,b\rangle\in \mathrm{BI}(2^2)$, 若 $\langle a\rangle\bigcap\langle b\rangle=1$, 则 $\mho_2(G)\leqslant Z(G)$. 但是若去掉 $\langle a\rangle\bigcap\langle b\rangle=1$ 这个条件, 该结论不一定成立. 例如广义四元数群 $\mathrm{Q}_{2^5}\in \mathrm{BI}(2^2)$, 但是 $\mho_2(\mathrm{Q}_{2^5})\nleqslant Z(\mathrm{Q}_{2^5})$. 然而我们有如下定理.

定理 11.7.24　设 $G\in \mathrm{BI}(2^2)$. 则 $\mho_3(G)\leqslant Z(G)$ 且 $\mho_2(G)$ 是交换群.

证明　设 $a,b\in G$, 其中 $|a|=2^m$, $|b|=2^n$. 下面证明 $[a^8,b]=[a,b^8]=1$ 且 $[a^4,b^4]=1$. 设 $H=\langle a,b\rangle$. 不失一般性, 假设 $m\geqslant n$.

若 $m\geqslant 5$, 由引理 11.7.23 可知, 存在 $b_1\in H$ 使得 $H=\langle a,b_1\rangle$ 且 $\langle a\rangle\bigcap\langle b_1\rangle=1$. 再由引理 11.7.19 得 $\mho_2(H)\leqslant Z(H)$. 因此 $[a^8,b]=[a,b^8]=1$ 且 $[a^4,b^4]=1$.

下设 $4\geqslant m\geqslant n$. 由引理 11.7.19 可知, 仅需考虑 $\langle a\rangle\bigcap\langle b\rangle\neq 1$ 的情形. 令 $\langle a^{2^k}\rangle=\langle a\rangle\bigcap\langle b\rangle$, 其中 $k\geqslant 1$. 再设 $\overline{H}=H/\langle a^{2^k}\rangle=\langle \bar{a},\bar{b}\rangle$. 引理 11.7.19 说明 $\exp(\overline{H}')\leqslant 4$ 且 $c(\overline{H})\leqslant 4$. 由此可得 $\mho_3(\overline{H})=1$. 因此 $\mho_3(\overline{H})\leqslant\langle a^{2^k}\rangle\leqslant Z(H)$. 于是 $[a^8,b]=[a,b^8]=1$. 若 $k\leqslant 2$, 则 $\langle b^4\rangle\leqslant\langle a^4\rangle$, 即 $[a^4,b^4]=1$. 若 $k=3$, 设 $H_1=\langle a^4,b\rangle$. 则由引理 11.7.5 可得 $\langle a^4\rangle\trianglelefteq H_1,\langle b\rangle\trianglelefteq H_1$. 于是 $c(H_1)\leqslant 2$ 且 $H'_1\leqslant\langle a^{2^3}\rangle$. 故 $[a^4,b^4]=1$, 定理得证. □

命题 11.7.25　设 $G\in \mathrm{BI}(2^2)$. 若 $|G|=2^{m+2}$ 且 $\exp(G)\geqslant 2^m$, 则 $|G'|\leqslant 2^3$.

证明　不妨设 G 非交换. 若 $\exp(G)=2^{m+1}$, 由定理 1.9.1 得, $G\cong \mathrm{M}_2(m+1,1)$ 或 $\mathrm{D}_{2^{m+2}}$, $\mathrm{Q}_{2^{m+2}}$, $\mathrm{SD}_{2^{m+2}}$. 若 $G\cong \mathrm{M}_2(m+1,1)$, 则 $|G'|=2$. 若 $G\cong \mathrm{D}_{2^{m+2}}$, $\mathrm{Q}_{2^{m+2}}$ 或 $\mathrm{SD}_{2^{m+2}}$, 则 $m\leqslant 3$. 因此 $|G'|\leqslant 2^3$.

若 $\exp(G)=2^m$, 如果 $m\geqslant 5$, 则存在 $a\in G$ 满足 $|a|=2^m$. 取 $b\in G\backslash\langle a\rangle$. 由引理 11.7.23 知, 存在 $b_1\in G$ 使得 $\langle a,b\rangle=\langle a,b_1\rangle$ 且 $\langle a\rangle\bigcap\langle b_1\rangle=1$. 若 $G=\langle a,b\rangle$, 由引理 11.7.19 可得 $|G'|\leqslant 2^3$. 若 $\langle a,b\rangle$ 是 G 的真子群, 则 $|b_1|=2$. 取 $b_2\in G\backslash\langle a,b_1\rangle$. 同理, 若 $G=\langle a,b_2\rangle$, $|G'|\leqslant 2^3$. 下设 $H_1=\langle a,b_1\rangle$ 和 $H_2=\langle a,b_2\rangle$ 都是 G 的真子群. 显然 $|H_1|=|H_2|=2^{m+1}$. 因为 $H_i\in \mathrm{BI}(2^2)(i=1,2)$, 故 $H_i\cong \mathrm{M}_{2^{m+1}}$ 或 $H_i\cong \mathrm{C}_{2^m}\times \mathrm{C}_2$. 于是 $\Omega_1(H_i)\cong \mathrm{C}_2\times \mathrm{C}_2$. 又 $G=\langle a,\Omega_1(H_1),\Omega_1(H_2)\rangle$ 且 $H_i\trianglelefteq G(i=1,2)$, 故 $G'\leqslant\langle\Omega_1(H_1),\Omega_1(H_2)\rangle$. 由于 $a^{2^{m-1}}\in H_i(i=1,2)$ 且 $\Omega_1(H_i)\trianglelefteq G$, 则 $|\langle\Omega_1(H_1),\Omega_1(H_2)\rangle|\leqslant 2^3$. 因此 $|G'|\leqslant 2^3$. 若 $m=4$, 易得 G 不是极大类群. 因而 $|G'|\leqslant 2^3$. 若 $m\leqslant 3$, 则 $|G|\leqslant 2^5$, 即可得 $|G'|\leqslant 2^3$. □

命题 11.7.26　设 2 群 G 存在指数是 2 的循环子群 $A=\langle a\rangle$. 若 $|a|=2^n\geqslant 2^4$, 则 G 不能由两个阶是 2^3 的元生成.

证明　仅需考虑 G 是非交换群. 则由定理 1.9.1 知, G 同构于 $\mathrm{M}_2(n,1)$, $\mathrm{D}_{2^{n+1}}$, $\mathrm{Q}_{2^{n+1}}$ 或 $\mathrm{SD}_{2^{n+1}}$. 若 G 同构于 $\mathrm{M}_2(n,1)$, 则 $\Omega_{n-1}(\mathrm{M}_2(n,1))$ 是 $\mathrm{M}_2(n,1)$ 的真子群, 因此这种情况不存在. G 也不能同构于 $\mathrm{D}_{2^{n+1}}$ 或 $\mathrm{Q}_{2^{n+1}}$, 这是因为所有阶是 2^3 的元都在 $\langle a\rangle$ 中. 若 $G\cong \mathrm{SD}_{2^{n+1}}$, 则 $G/Z(G)\cong \mathrm{D}_{2^n}$. 但是 $G/Z(G)$ 不可能由两个 4 阶元生成, 即 G 不能由两个阶是 2^3 的元生成. □

定理 11.7.27　设 $a,b\in G\in \mathrm{BI}(2^2)$. 则 $|\langle[a,b]\rangle^G|\leqslant 2^4$, $[a,b]^8=1$, 因此

$c(G) \leqslant 5$.

证明 设 $|a| = 2^m$, $|b| = 2^n$ 且 $c = [a, b]$. 不妨设 $m \geqslant n$.

设 $a \in \langle b\rangle^G$. 由命题 11.7.25 可得 $|(\langle b\rangle^G)'| \leqslant 2^3$. 因为 $c \in (\langle b\rangle^G)'$, 故 $|\langle c\rangle^G| \leqslant 2^3$ 且 $c^8 = 1$. 不妨设 $a \notin \langle b\rangle^G$ 且 $b \notin \langle a\rangle^G$.

若 $\langle a\rangle \bigcap \langle b\rangle = 1$, 设 $A = \langle a\rangle^G \bigcap \langle b\rangle^G$. 则 $|A| \leqslant 2^4$. 若 $|A| \geqslant 2^3$, 则 $a^{2^{m-1}}$, $b^{2^{n-1}} \in A$. 因此 $|\Omega_1(A)| \geqslant 4$, 进而可得 $\exp(A) \leqslant 2^3$. 显然当 $|A| \leqslant 2^2$ 也成立. 在此种情形下, 结论成立. 下设 $\langle a\rangle \bigcap \langle b\rangle \neq 1$. 依照 m 的取值分三种情形讨论.

(1) $m \geqslant 5$: 由引理 11.7.23 可知, 存在 $b_1 \in H = \langle a, b\rangle$ 使得 $H = \langle a, b_1\rangle$ 且 $\langle a\rangle \bigcap \langle b_1\rangle = 1$. 同上可得 $|\langle [a, b_1]\rangle^G| \leqslant 2^4$ 且 $\exp(\langle [a, b_1]\rangle^G) \leqslant 2^3$. 因此 $|\langle c\rangle^G| \leqslant 2^4$ 且 $c^8 = 1$.

(2) $m \leqslant 3$: 若 $m \leqslant 2$, 则 $|\langle a\rangle^G| \leqslant 2^4$. 易得 $|\langle c\rangle^G| \leqslant 2^3$. 设 $m = 3$. 则 $|\langle a\rangle^G| \leqslant 2^5$. 于是 $|\langle c\rangle^G| \leqslant 2^4$. 若 $\langle c\rangle^G$ 是阶为 2^4 的循环群, 由 $\langle a\rangle^G$ 是非循环群可得 $|\langle a\rangle^G : \langle c\rangle^G| = 2$. 又由命题 11.7.26 得, $\langle a\rangle^G$ 不可能由阶是 2^3 的元生成, 这与 $|a| = 2^3$ 相矛盾. 因此 $\exp(\langle c\rangle^G) \leqslant 2^3$, 即 $c^8 = 1$.

(3) $m = 4$: 若 $|b| \leqslant 2^3$, 则 $|\langle a\rangle^G \bigcap \langle b\rangle^G| \leqslant 2^4$. 因此 $|\langle c\rangle^G| \leqslant 2^4$. 下面仅考虑 $|a| = |b| = 2^4$. 设 $H = \langle a, b\rangle$.

(3.1) $\langle a^4\rangle \leqslant \langle a\rangle \bigcap \langle b\rangle$: 若 $|\langle a\rangle^H : \langle a\rangle| \leqslant 2$, 由引理 11.7.21 知, 存在 $b_1 \in H$ 使得 $H = \langle a, b_1\rangle$ 且 $|b_1| \leqslant 2^3$. 类似可得 $|\langle [a, b_1]\rangle^G| \leqslant 2^4$ 且 $c^8 = 1$. 因此可设 $|\langle a\rangle^H : \langle a\rangle| = 4$ 且 $|\langle b\rangle^H : \langle b\rangle| = 4$. 再设 $H = \langle a\rangle^H \langle b\rangle^H = \langle a\rangle^G \langle b\rangle^G \trianglelefteq G$, $\overline{H} = H/\langle a^4\rangle$. 由 $\overline{H} \in \mathrm{BI}(2^2)$ 可得 $|\overline{H}| \leqslant 2^6$. 下面将证明 $|H'| \leqslant 2^4$.

若 $|\overline{H}| = 2^6$, 则 $|\langle \bar{a}\rangle^{\overline{H}} \bigcap \langle \bar{b}\rangle^{\overline{H}}| = 4$ 且 $|\overline{H}'| \leqslant 4$. 因此 $|H'| \leqslant 2^4$. 若 $|\overline{H}| = 2^5$, 则 $|H/\langle a^8\rangle| = 2^6$. 由命题 11.7.26 可知, $H/\langle a^8\rangle$ 不是极大类群. 由此可得 $|(H/\langle a^8\rangle)'| \leqslant 2^3$, 即 $|H'| \leqslant 2^4$. 若 $|\overline{H}| \leqslant 2^4$, 易得 $|\overline{H}'| \leqslant 4$ 且 $|H'| \leqslant 2^4$.

我们断定 H' 不是阶为 2^4 的循环群. 若否, $H' = \langle c\rangle$, 且 $|c| = 2^4$. 因而 $c^a = c^k$, 其中 $(k, 2) = 1$ 且 $1 \leqslant k \leqslant 2^4$. 若 $a^4 \notin \langle c\rangle \bigcap \langle a\rangle$, 则 $|\bar{c}| \geqslant 2^3$. 由此可得 $|\overline{H}| \geqslant 2^6$, 与 $|\langle \bar{a}\rangle^{\overline{H}} \bigcap \langle \bar{b}\rangle^{\overline{H}}| = 4$ 相矛盾. 因此 $c^4 \in \langle a\rangle$ 且 $(c^4)^a = c^{4k} = c^4$. 因为 $a^4 \in Z(H)$, 故 $[a^4, b] = 1$. 注意此时 $[a^4, b] = [a, b]^{a^3}[a, b]^{a^2}[a, b]^a[a, b]$, 于是 $c^{k^3}c^{k^2}c^k c = c^{k^3+k^2+k+1} = 1$. 从而可得

$$\begin{cases} k^3 + k^2 + k + 1 \equiv 0 \pmod{2^4}, \\ 4k \equiv 4 \pmod{2^4}. \end{cases} \tag{11.2}$$

显然由 $(k, 2) = 1$ 且 $1 \leqslant k \leqslant 2^4$ 可知方程组无解. 故 H' 不是阶是 2^4 的循环群. 这说明 $c^8 = 1$ 且 $|\langle c\rangle^G| \leqslant 2^4$.

(3.2) $\langle a^8\rangle = \langle a\rangle \bigcap \langle b\rangle$: 由定理 11.7.24 可知 $a^8 \in Z(G)$. 设 $\overline{G} = G/\langle a^8\rangle$. 因为 $\overline{H} = \langle \bar{a}, \bar{b}\rangle \in \mathrm{BI}(2^2)$ 且 $\langle \bar{a}\rangle \bigcap \langle \bar{b}\rangle = 1$, 由引理 11.7.19 可得 $|\bar{c}| \leqslant 2^2$. 由此

可得 $c^8=1$. 若 $|\langle c\rangle^G|=2^5$, 则 $|\langle c\rangle^G\bigcap\langle a\rangle|\geqslant 2^3$ 且 $|\langle c\rangle^G\bigcap\langle b\rangle|\geqslant 2^3$. 由此可得 $\langle c\rangle^G=\langle a\rangle^G\bigcap\langle b\rangle^G=\langle a^2,b^2\rangle$. 进而 $\langle a\rangle^G=\langle a,b^2\rangle$ 且 $\langle b\rangle^G=\langle b,a^2\rangle$. 故 $H=\langle a,b\rangle=\langle a\rangle^G\langle b\rangle^G\trianglelefteq G$. 再由引理 11.7.19 可得, $|\overline{H}'|\leqslant 2^3$ 且 $\exp(\overline{H}')\leqslant 4$. 因此 $|H'|\leqslant 2^4$ 且 $H'\trianglelefteq G$, 矛盾. 故定理的结论成立. □

推论 11.7.28　设 $G\in \mathrm{BI}(2^2)$. 则 $\exp(G')\leqslant 2^3$.

证明　设 $c=[a_1,b_1]$, $d=[a_2,b_2]$, 其中 $a_1,a_2,b_1,b_2\in G$. 由定理 11.7.27 可得 $c^8=d^8=1$, $|\langle c\rangle^G|\leqslant 2^4$ 且 $|\langle d\rangle^G|\leqslant 2^4$. 设 $x=c^md^n$. 下面证明 $x^8=1$.

设 $H=\langle c\rangle^G, K=\langle d\rangle^G$. 若 $|H\bigcap K|\leqslant 4$, 则 $x^8=(c^m)^8(d^n)^8c_2^{\binom{8}{2}}c_3^{\binom{8}{3}}=1$, 其中 $c_2,c_3\in H\bigcap K$. 若 $|H\bigcap K|=8$, 则 $|HK|\leqslant 2^5$. 如果存在元 $g\in HK$ 使得 $|g|=2^4$, 那么 HK 是交换群, 或 $HK\cong \mathrm{M}_2(4,1)$ 或 HK 是极大类群. 若 HK 是交换群或 $HK\cong \mathrm{M}_2(4,1)$, 则 $\Omega_3(HK)$ 是 HK 的真子群, 即可得 $\exp(HK)\leqslant 2^3$. 由定理 11.7.27 知, $HK\leqslant\Omega_3(HK)$, 矛盾. 若 HK 是极大类群, 则 $c(HK)=4$. 但是由 $HK\leqslant G'$ 且 $c(G)\leqslant 5$ 可得 $c(HK)\leqslant 3$, 矛盾. 因此对任意 $g\in HK$ 都有 $g^8=1$. 由 Hall-Petrescu 恒等式可得 $\exp(G')\leqslant 2^3$. □

文献 [139] 对于正则 $\mathrm{BI}(p^m)$ 群的性质及两个 $\mathrm{BI}(p^m)$ 群的直积何时为 $\mathrm{BI}(p^m)$ 群等问题也给出了一些结果. 在此不再赘述.

11.8　非正规子群的正规化子较小的 p 群

设 G 是有限 p 群, H 是 G 的真子群. 一个众所周知的结论是: $H<N_G(H)$. 换句话说, $|N_G(H):H|\geqslant p$. 引起许多群论学者感兴趣的问题是: 若 p 群 G 的所有非正规子群 H 均有 $|N_G(H):H|=p$, 那么 G 的结构如何呢? 黎先华等在文献 [134] 及张勤海等在文献 [277] 分别独立地分类了这样的群. 进一步地, 文献 [277] 还分类了所有非正规子群 H 均有 $|N_G(H):H|=p^i$ 的 p 群 G, 这里 i 是任意一个固定的正整数. Berkovich 和 Janko 在他们的 p 群专著 [28] 中的第 138 节对于 $i=1$ 的情况也给出了分类. 另外, 他们也分类了所有非正规循环子群 H 均有 $|N_G(H):H|=p$ 的 p 群 G. 沿着这个方向, 张小红等在 [281] 确定了所有非正规循环子群 H 均有 $|N_G(H):H|\leqslant p^w$ 的奇数阶 p 群 G 的阶并在 $w=2$ 的情形下分类了这样的 p 群. 张军强在文献 [262] 分类了所有非正规子群 H 均有 $N_G(H)/H$ 循环的 p 群 G. 有趣的是, 这样的群与 Blacburn 等在文献 [34] 研究的 n-单列子群 (n-uniserial subgroups)及单列嵌入子群 (uniserially embedded subgroups)有密切联系. p 群 G 的子群 H 称为 ***n*-单列子群**, 若对每个 $i\in\{1,2,\cdots,n\}$, G 有唯一的子群 K_i 使得 $H\leqslant K_i$ 且 $|K_i:H|=p^i$. 在此情况下, 若 G 的包含 H 的子群构成一个链, 则称 H 是单列嵌入于 G. 换句话说, 仅有唯一的极大链连接 G 与 H. 作为文献 [262] 的推论, 非正规子群均为 1 单列的 p 群 $(p\neq 2)$ 及非正规子群均为单列嵌

入的 p 群被分类.

11.8.1 非正规子群在其正规化子中的指数为 p 的 p 群

设 G 为有限 p 群. 若 G 具有性质: 对 G 的所有非正规子群 H 均有 $|N_G(H):H|=p^i$, 则称 G 为 $\mathcal{S}_i$ 群 (或 $G\in\mathcal{S}_i$). 这里 i 是固定的正整数. 对于每个 i，文献 [277] 分类了 $\mathcal{S}_i$ 群. 本节介绍 $\mathcal{S}_1$ 群的分类. 我们观察到, 若 $|G|\leqslant p^3$, 则 G 是 $\mathcal{S}_1$ 群. 不妨设 $\mathcal{S}_1$ 群的阶大于 p^3.

引理 11.8.1 (1) 若 $G\in\mathcal{S}_1$, $H\leqslant G$, 则 $H\in\mathcal{S}_1$;

(2) 若 $G\in\mathcal{S}_i$, $N\trianglelefteq G$, 则对于 $i\geqslant 1$, $G/N\in\mathcal{S}_i$.

证明 (1) 设 $H\leqslant G$ 且 $K\leqslant H$. 若 $K\ntrianglelefteq H$, 则 $K\ntrianglelefteq G$. 由假设条件得 $|N_G(K):K|=p$. 因为 $|N_H(K):K|\leqslant|N_G(K):K|$ 且 $K<N_H(K)$, 故 $|N_H(K):K|=p$. 因而 $H\in\mathcal{S}_1$.

(2) 设 $N\trianglelefteq G$ 且 $H/N\ntrianglelefteq G/N$. 则 $H\ntrianglelefteq G$. 由此可得

$$|N_{G/N}(H/N):H/N|=|N_G(H)/N:H/N|=|N_G(H):H|=p^i.$$

于是 $G/N\in\mathcal{S}_i$. □

引理 11.8.2 设 G 是奇阶内交换 p 群且 $|G|\geqslant p^4$. 若 $G\in\mathcal{S}_1$, 则 $G\cong \mathrm{M}_p(2,2)$.

证明 由定理 1.7.10 知, $G\cong\mathrm{M}_p(n,m,1)$ 或 $G\cong\mathrm{M}_p(n,m)$. 若 $G\cong\mathrm{M}_p(n,m,1)$, 由 $|G|\geqslant p^4$ 的假设推出 $n+m+1\geqslant 4$. 又由 $n\geqslant m$ 得 $n\geqslant 2$. 令

$$G=\langle a,b,c\mid a^{p^n}=b^{p^m}=c^p=1,[a,b]=c,[a,c]=[b,c]=1\rangle.$$

明显地, $\langle b\rangle\ntrianglelefteq G$. 另一方面, $N_G(\langle b\rangle)\geqslant\langle a^p\rangle\times\langle c\rangle\times\langle b\rangle$. 于是 $|N_G(\langle b\rangle):\langle b\rangle|\geqslant p^n\geqslant p^2$, 矛盾. 于是 $G\cong\mathrm{M}_p(n,m)$. 若 $n\geqslant 3$, 令

$$G=\langle a,b\mid a^{p^n}=b^{p^m}=1,[a,b]=a^{p^{n-1}}\rangle.$$

明显地, $\langle b\rangle\ntrianglelefteq G$. 另一方面, $N_G(\langle b\rangle)\geqslant\langle a^p\rangle\times\langle b\rangle$. 于是 $|N_G(\langle b\rangle):\langle b\rangle|\geqslant p^{n-1}\geqslant p^2$, 矛盾. 故 $n=2$. 若 $m\geqslant 3$, 令

$$G=\langle a,b\mid a^{p^2}=b^{p^m}=1,[a,b]=a^p\rangle,$$

其中 $\langle ab^{p^{m-2}}\rangle\ntrianglelefteq G$, $o(\langle ab^{p^{m-2}}\rangle)=p^2$. 但是 $N_G(\langle ab^{p^{m-2}}\rangle)=\langle a\rangle\times\langle b^p\rangle$. 故

$$|N_G(\langle ab^{p^{m-2}}\rangle):\langle ab^{p^{m-2}}\rangle|\geqslant p^{m-1}\geqslant p^2.$$

矛盾. 故 $m=2$. 由此得 $G\cong\mathrm{M}_p(2,2)$. □

定理 11.8.3 设 G 是有限 p 群, $p>2$ 且 $|G|\geqslant p^4$. 则 $G\in\mathcal{S}_1$ 当且仅当 G 交换或 $G\cong\mathrm{M}_p(2,2)$.

证明　$\Longleftarrow$: 若 G 交换, 结论明显成立. 设 $G \cong \mathrm{M}_p(2,2)$. 因为 $\Omega_1(G)=Z(G)$, 故 G 的所有 p 阶子群正规. 明显地, G 的所有 p^3 阶子群正规. 故若 $H \ntrianglelefteq G$, 则 $|H|=p^2$. 由此可得 $H<N_G(H)<G$. 于是 $|N_G(H):H|=p$. 即 $G\in\mathcal{S}_1$.

$\Longrightarrow$: 对 $|G|$ 作归纳. 若 $|G|=p^4$ 且 $G\in\mathcal{S}_1$, 易证 G 交换或 $G\cong \mathrm{M}_p(2,2)$. 结论成立. 设结论对阶 $<|G|$ 的群成立. 因为 G 是 p 群, 存在 p 子群 N 使得 $N\leqslant G'\bigcap Z(G)$. 由引理 11.8.1 及归纳假设得, G/N 交换或 $G/N\cong \mathrm{M}_p(2,2)$.

若 $G/N\cong \mathrm{M}_p(2,2)$, 则

$$|(G/N)'|=|G'N/N|=|G'/G'\bigcap N|=|G'/N|=p.$$

于是 $|G'|=p^2$. 由定理 6.2.1 得

$$G\cong\langle a,b\mid a^{p^3}=b^{p^2}=1,[a,b]=a^p\rangle.$$

于是 $\langle b^p\rangle\ntrianglelefteq G$, $|\langle b^p\rangle|=p$. 但是 $N_G(\langle b^p\rangle)=\langle a^p,b\rangle\cong \mathrm{M}_p(2,2)$. 于是 $|N_G(\langle b^p\rangle):\langle b^p\rangle|=p^3$, 矛盾.

若 G/N 交换, 则 G 交换或非交换. 若 G 非交换, 则

$$|(G/N)'|=|G'N/N|=|G'/G'\bigcap N|=|G'/N|=1.$$

故 $|G'|=p$. 由定理 10.1.2 得

$$G\cong A_1*A_2*\cdots*A_sZ(G),$$

其中 A_i 内交换. 不妨设 $G=A_1*K$. 若 $K\nleqslant A_1$, 则存在 $g\in K\backslash A_1$ 使得对任意的 $H\ntrianglelefteq A_1$ 均有 $N_G(H)\geqslant\langle N_{A_1}(H),g\rangle$. 于是 $|N_G(H):H|\geqslant p^2$, 矛盾. 由此可得 $K\leqslant A_1$. 即 $G=A_1$. 由引理 11.8.2 即得 $G\cong \mathrm{M}_p(2,2)$. □

引理 11.8.4　设 G 是极大类 2 群. 则

(i) $G/Z(G)\cong \mathrm{D}_{2^{n-1}}$;

(ii) G 的每个极大子群或循环或极大类.

证明　由 [89] 中的III, 定理 11.9b 可知, G 同构于 D_{2^n}, Q_{2^n} 或 SD_{2^n} 中之一. 简单的验证即得所证. □

定理 11.8.5　设 G 是 2^n 阶群. 则 $G\in\mathcal{S}_1$ 当且仅当 G 是下列互不同构的群之一.

(Ⅰ) Dedekind 2 群;

(Ⅱ) 极大类 2 群;

(Ⅲ) $\langle a,b\mid a^{2^{n-2}}=b^4=1,[a,b]=a^{-2}\rangle$;

(Ⅳ) $\langle a,b\mid a^{2^{n-2}}=b^4=1,[a,b]=a^{-2+2^{n-3}}\rangle$.

证明 $\Longleftarrow$: 若 G 是极大类 2 群, 下证 $G\in\mathcal{S}_1$. 设 $H\ntrianglelefteq G$. 若 $|G:H|=2^2$, 则 $|N_G(H):H|=2$. 不妨设 $|G:H|\geqslant 2^3$. 设 G 是极小阶反例. 则存在 $H\ntrianglelefteq G$ 使得 $|N_G(H):H|>2$. 因为 $N_G(H)<G$, 存在 $M\lessdot G$ 使得 $N_G(H)\leqslant M$. 由引理 11.8.4 可知, M 循环或极大类. 若 M 循环, 则 $H\trianglelefteq G$, 矛盾. 故 M 是极大类的. 若 $H\trianglelefteq M$, 由 $|G:H|\geqslant 2^3$ 得 $|M:H|\geqslant 2^2$. 由定理 1.11.8 易知, H char $M\trianglelefteq G$. 由此可得 $H\trianglelefteq G$, 矛盾. 于是 $H\ntrianglelefteq M$. 因为 G 极小阶反例, 故 $|N_M(H):H|=2$. 另一方面, $N_M(H)=N_G(H)\bigcap M=N_G(H)$. 故 $|N_G(H):H|=2$, 又是矛盾. 故极小反例不存在.

若 G 是群 (III), 则 $G/\langle b^2\rangle=\langle\overline{a},\overline{b}\mid\overline{a}^{2^{n-2}}=\overline{b}^2=1,[\overline{a},\overline{b}]=\overline{a}^{(-2)}\rangle\cong \mathrm{D}_{2^{n-1}}$. 令 $H\ntrianglelefteq G$. 则 $\langle b^2\rangle\leqslant H$. 若否, 令 $K=\langle a,b^2\rangle$. 则 $H\leqslant K$. 观察到,

$$H\leqslant K\Longleftrightarrow G\backslash H\supseteq G\backslash K\Longleftrightarrow \forall g\in G\backslash K\Longrightarrow g\in G\backslash H\Longleftrightarrow \forall g\in G\backslash K\Longrightarrow g\notin H.$$

因为 G 的每个元具有 b^ja^i 的形式, $j=0,1,2,3$, 故我们只需证 $ba^i, b^{-1}a^i\notin H$. 简单的计算可知, 对任意的 i 有

$$(ba^i)^2=ba^iba^i=b^2(a^b)^ia^i=b^2.$$

故 $ba^i\notin H$. 同理,

$$(b^{-1}a^i)^2=b^{-1}a^ib^{-1}a^i=b^3a^ib^3a^i=ba^iba^i=b^2.$$

故 $b^{-1}a^i\notin H$. 于是 $H\leqslant K=\langle a,b^2\rangle$. 进一步地, $\langle a,b^2\rangle$ 的所有循环子群在 G 中正规. 事实上, 对于 $g\in\langle a,b^2\rangle$, 令 $g=a^ib^{2j}$. 则

$$g^a=(a^ib^{2j})^a=g,\quad g^b=(a^ib^{2j})^b=(a^b)^ib^{2j}=a^{-i}b^{2j}=g^{-1}.$$

故 $\langle g\rangle\trianglelefteq G$. 由此可得 $H\trianglelefteq G$, 矛盾. 故 $\langle b^2\rangle\leqslant H$.

因为 $H\ntrianglelefteq G$, 故 $\overline{H}\ntrianglelefteq\overline{G}$. 又 $\overline{G}$ 是极大类的, 故 $|N_{\overline{G}}(\overline{H}):\overline{H}|=2$. 于是 $|N_G(H):H|=|N_{\overline{G}}(\overline{H}):\overline{H}|=2$, 即群 (III) 属于 $\mathcal{S}_1$.

设 G 是群 (IV), 考虑 $G/\langle b^2\rangle$ 和 $G/\langle a^{2^{n-3}}b^2\rangle$. 则

$$G/\langle b^2\rangle=\langle\overline{a},\overline{b}\mid\overline{a}^{2^{n-2}}=\overline{b}^2=1,[\overline{a},\overline{b}]=\overline{a}^{(-2+2^{n-3})}\rangle\cong\mathrm{SD}_{2^{n-1}},$$

$$G/\langle a^{2^{n-3}}b^2\rangle=\langle\overline{a},\overline{b}\mid\overline{a}^{2^{n-2}}=1,\overline{b}^2=\overline{a}^{2^{n-3}},[\overline{a},\overline{b}]=\overline{a}^{(-2+2^{n-3})}\rangle\cong\mathrm{SD}_{2^{n-1}}.$$

令 $H\ntrianglelefteq G$. 下证 $\langle b^2\rangle\leqslant H$ 或 $\langle a^{2^{n-3}}b^2\rangle\leqslant H$. 若否, 令 $K=\langle a,b^2\rangle$. 则 $H\leqslant K$. 又

$$H\leqslant K\Longleftrightarrow G\backslash H\supseteq G\backslash K\Longleftrightarrow \forall g\in G\backslash K\Longrightarrow g\in G\backslash H\Longleftrightarrow \forall g\in G\backslash K\Longrightarrow g\notin H.$$

这与 G 为群 (III) 的论证类似可得 $H\trianglelefteq G$. 矛盾. 从而 $\langle b^2\rangle\leqslant H$ 或 $\langle a^{2^{n-3}}b^2\rangle\leqslant H$.

因为 $H \ntrianglelefteq G$, 故 $\overline{H} \ntrianglelefteq \overline{G}$. 又 $\overline{G}$ 是极大类的, 故 $|N_{\overline{G}}(\overline{H}):\overline{H}| = 2$. 于是 $|N_G(H):H| = |N_{\overline{G}}(\overline{H}):\overline{H}| = 2$, 即群 (IV) 属于 $\mathcal{S}_1$.

$\Longrightarrow$: 分两种情形讨论.

情形 1　$d(G) \geqslant 3$.

设 $G \in \mathcal{S}_1$ 且 G 非交换. 下证 G 是非交换的 Dedekind 群. 设 G 是极小阶反例. 因为 $\Phi(G) \neq 1$, 取 $N \leqslant \Phi(G)$ 使得 $|N| = 2$ 且 $N \trianglelefteq G$. 于是 $d(G/N) = d(G) \geqslant 3$. 由引理 11.8.1, G/N 是非交换的 Dedekind 群. 因为 G 是极小阶反例, 故存在 $a \in G$ 使得 $\langle a\rangle \ntrianglelefteq G$. 从而 $N \bigcap \langle a\rangle = 1$. 因为 $N_G(\langle a\rangle) \geqslant \langle N, a\rangle = N \times \langle a\rangle$, 由假设可得 $|N_G(\langle a\rangle):\langle a\rangle| = 2$. 于是 $N_G(\langle a\rangle) = N \times \langle a\rangle$. 因为 G/N 是 Dedekind 2 群, 故 $(N \times \langle a\rangle)/\langle a\rangle \trianglelefteq G/N$. 于是 $N \times \langle a\rangle \trianglelefteq G$.

下面计算 $|\{\langle a\rangle^g | g \in G\}|$. 首先证明: $|\{\langle a\rangle^g | g \in G\}| = |G:N_G(\langle a\rangle)| \geqslant 2^2$. 因为 $d(G) \geqslant 3$, 故 $|G/\langle a, \Phi(G)\rangle| \geqslant 2^2$. 令 $\overline{G} = G/N_G(\langle a\rangle)$. 则

$$\Phi(\overline{G}) = \Phi(G/N_G(\langle a\rangle)) = (\Phi(G)N_G(\langle a\rangle))/N_G(\langle a\rangle),$$

$$\Phi(G)N_G(\langle a\rangle) = \Phi(G)(N \times \langle a\rangle) = \Phi(G)\langle a\rangle = \langle a, \Phi(G)\rangle.$$

于是 $\overline{G}/\Phi(\overline{G}) \cong G/(\langle a, \Phi(G)\rangle)$. 又 $|G:(\langle a, \Phi(G)\rangle)| \geqslant 2^2$, 故 $|\overline{G}/\Phi(\overline{G})| \geqslant 2^2$. 即 $d(\overline{G}) \geqslant 2$. 从而 $|\overline{G}| \geqslant 2^2$. 即 $|G:N_G(\langle a\rangle)| \geqslant 2^2$. 另一方面, 因为 $\langle a\rangle \leqslant N \times \langle a\rangle$, 故 $\langle a\rangle^g \leqslant (N \times \langle a\rangle)^g = N \times \langle a\rangle$. 于是 $\langle a\rangle^g \lessdot N \times \langle a\rangle$. 又 $d(N \times \langle a\rangle) = 2$, 故 $N \times \langle a\rangle$ 有三个极大子群. 从而 $|\{\langle a\rangle^g | g \in G\}| \leqslant 2$. 这是一个矛盾. 这说明极小阶反例不存在.

情形 2　$d(G) \leqslant 2$.

对 $|G|$ 作归纳. 若 $|G| = 2^4$ 且 $G \in \mathcal{S}_1$, 易证 G 是 Dedekind 群, 极大类群或 $\mathrm{M}_2(2,2)$. 结论成立. 假设结论对阶 $< |G|$ 的群成立. 因为 G 是 2 群, 存在 $N \leqslant G' \bigcap Z(G)$ 且 $|N| = 2$. 由归纳假设, G/N 是定理中的群之一.

若 G/N 交换, 与 $p > 2$ 的论证类似可证, G 交换, 或 $G \cong \mathrm{Q}_8$, D_8 或 $\mathrm{M}_2(2,2)$.

若 G/N 是极大类的, 由 [89] 中的III, 引理 14.2 可知, $|(G/N)'| = 2^{n-2}$. 因为

$$(G/N)' = G'N/N \cong G'/G' \bigcap N = G'/N,$$

故 $|G'/N| = 2^{n-2}$. 于是 $|G'| = 2^{n-1}$. 由此可得 $|G/G'| = 4$. 从而 G 是极大类的.

若 G/N 是群 (III), 即 $\overline{G} \cong \langle \overline{a}, \overline{b} \mid \overline{a}^{2^{n-2}} = \overline{b}^4 = 1, [\overline{a}, \overline{b}] = \overline{a}^{(-2)}\rangle$. 设 $N = \langle x\rangle$. 则

$$G = \langle a, b \mid a^{2^{n-2}} = x^i, b^4 = x^j, [a,b] = a^{-2}x^k, x^2 = 1, [x,a] = [x,b] = 1\rangle.$$

令 $K = \langle a^{-2}x^k\rangle$. 易证 G/K 交换. 于是 $G' \leqslant K$. 但是 $K \leqslant G'$. 故 $G' = K$. 即 G' 循环. 因为 $|G'| = 2^{n-2}$, 由 $[a,b]^{2^{n-2}} = 1$ 推出 $o(a) = 2^{n-1}$ 且 $N = \langle a^{2^{n-2}}\rangle$. 于是我们得到下列可能的群:

(a1) $\langle a, b \mid a^{2^{n-1}} = 1, b^4 = 1, [a, b] = a^{-2} \rangle$;

(a2) $\langle a, b \mid a^{2^{n-1}} = 1, b^4 = 1, [a, b] = a^{-2+2^{n-2}} \rangle$;

(a3) $\langle a, b \mid a^{2^{n-1}} = 1, b^4 = a^{2^{n-2}}, [a, b] = a^{-2} \rangle$;

(a4) $\langle a, b \mid a^{2^{n-1}} = 1, b^4 = a^{2^{n-2}}, [a, b] = a^{-2+2^{n-2}} \rangle$.

明显地, 群 (a1) 同构于群 (III); 群 (a2) 同构于群 (IV). 对于群 (a3), 令 $H = \langle a^{2^{n-3}} b^2 \rangle$. 则 $|H| = 2$ 且 $H \ntrianglelefteq G$, $N_G(H) = \langle a, b^2 \rangle \lessdot G$. 于是 $|N_G(H) : H| \geqslant 2^3$, 矛盾. 对于群 (a4), 令 $a' = ab^2$, $b' = b$. 则 (a4) $\cong$ (a3).

若 G/N 是群 (IV), 类似于上面的论证可知, 没有新的群出现. □

11.8.2 非正规子群在其正规化子中的指数不超过 p^2 的 p 群

张小红等在 [281] 称非正规循环子群在其正规化子中的指数不超过 p^w 的有限 p 群为 $\mathcal{N}_{p^m}$ 群. 文献 [281] 给出了 $\mathcal{N}_{p^m}$ 群的阶的上限并在 $p \neq 2$ 的情形下分类了 $\mathcal{N}_{p^2}$ 群. 本节介绍他们的工作.

首先给出 $\mathcal{N}_{p^m}$ 群的某些性质, 鉴于篇幅所限, 这里略去其证明.

引理 11.8.6 设 G 是 $\mathcal{N}_{p^m}$ 群. 则

(1) $r(G) \leqslant m + 1$;

(2) $Z(G)$ 不循环除非 G 是极大类 2 群.

引理 11.8.7 设 G 是 $\mathcal{N}_{p^m}$ 群, N 是 G 的 p^n 阶交换子群, 其中 $n \geqslant m+1$. 若对于 $x \in N$ 有 $o(x) \leqslant p^{n-m-1}$, 则 $\langle x \rangle \trianglelefteq G$.

引理 11.8.8 设 G 是奇阶 $\mathcal{N}_{p^m}$ 群, N 是 G 的极大阶的交换正规子群. 若对于非负整数 s 有 $|N| = p^{2m+s}$, 则

(1) $\Omega_1(N) \leqslant Z(G)$;

(2) 存在 $g \in G \setminus N$ 使得 g 在 N 上诱导一个 p 阶自同构. 进一步地, $\mho_1(N) < C_G(g)$, $c(\langle N, g \rangle) = 2$ 且 $\exp(\langle N, g \rangle') = p$.

定理 11.8.9 设 G 是奇阶 $\mathcal{N}_{p^m}$ 群, N 是 G 的交换正规子群. 则

(1) $|N| \leqslant p^{2m+1}$;

(2) $|G| \leqslant p^{(2m+1)(m+1)}$.

下面分类奇阶 $\mathcal{N}_{p^2}$ 群 G. 我们观察到, 若 $|G| = p^n \leqslant p^{m+2}$, 则 G 是 $\mathcal{N}_{p^m}$ 群. 另一方面, 若 G 是 Dedekind p 群, 则对于任意正整数 m, G 也是 $\mathcal{N}_{p^m}$ 群. 故只需考虑非 Dedekind 的且阶不小于 p^{m+3} 的 $\mathcal{N}_{p^m}$ 群. 于是可设 $\mathcal{N}_{p^2}$ 群的阶不小于 p^5.

引理 11.8.10 设 G 是 p 群. 若 $|G| \geqslant p^7$, 则 G 有一个 p^4 阶的交换正规子群.

证明 设 R 是 G 的 p^2 阶正规子群. 因为 $G/C_G(R) \lesssim \mathrm{Aut}(R)$ 且 $|G| \geqslant p^7$, 故 $|C_G(R)| \geqslant p^6$. 于是存在 G 的 p^3 阶正规子群 H 使得 $R < H < C_G(R)$. 显然 H 交换. 用 H 替换 R, 同样的论证可得 $|C_G(H)| \geqslant p^4$. 于是结论推出. □

引理 11.8.11 设 G 是 $\mathcal{N}_{p^2}$ 群, N 是 G 的极大阶的交换正规子群. 若 $|G| \geqslant p^6$, 则 $|N| \geqslant p^4$.

证明 由引理 11.8.10 和 [247] 中的定理 7.6.2 可知, 仅需证当 $|G| = p^6$ 时, G 有 p^4 阶交换子群.

由引理 11.8.6(2) 知, $Z(G)$ 不循环. 从而 $|Z(G)| \geqslant p^2$. 若 $|Z(G)| \geqslant p^3$, 则 G 有 p^4 阶交换子群. 若 $|Z(G)| = p^2$ 且存在 $g \in G$ 使得 $g^p \notin Z(G)$, 则 $Z(G)\langle g\rangle$ 是 G 的 p^4 阶交换子群. 设 $|Z(G)| = p^2$ 且对任意的 $g \in G \setminus Z(G)$ 有 $g^p \in Z(G)$. 则 $|G/Z(G)| = p^4$ 且 $\exp(G/Z(G)) = p$. 由 [247] 中的定理 2.6.4 可知, $G/Z(G)$ 同构于下列群之一: C_p^4, $\mathrm{M}_p(1,1,1) \times \mathrm{C}_p$ 或

$$\langle a, b, c, d \mid a^p = b^p = c^p = d^p = 1, [a, b] = c, [c, a] = 1, [c, b] = d\rangle.$$

令 $Z(G) = \langle e\rangle \times \langle f\rangle \cong \mathrm{C}_p \times \mathrm{C}_p$.

设 $G/Z(G) \cong \mathrm{C}_p^4 = \langle \overline{a}\rangle \times \langle \overline{b}\rangle \times \langle \overline{c}\rangle \times \langle \overline{d}\rangle$. 则 $G = \langle a, b, c, d, e, f\rangle$. 清楚地, $[a, b]$, $[a, c]$ 和 $[a, d] \in Z(G)$. 若 $[a, b] = 1$, 则 $\langle a\rangle\langle b\rangle Z(G)$ 是 G 的 p^4 阶交换子群. 设 $[a, b] = e$, $[a, c] = f$ 和 $[a, d] = e^i f^j$ $(p \nmid ij)$. 令 $b_1 = b^i$ 和 $c_1 = c^j$. 则 $[a, b_1c_1d^{-1}] = 1$. 从而 $\langle a\rangle\langle b_1c_1d^{-1}\rangle Z(G)$ 是 G 的 p^4 阶交换子群.

若 $G/Z(G) \cong \mathrm{M}_p(1,1,1) \times \mathrm{C}_p = \langle \overline{a}, \overline{b}, \overline{c}\rangle \times \langle \overline{d}\rangle$ 或

$$\langle \overline{a}, \overline{b}, \overline{c}, \overline{d} \mid \overline{a}^p = \overline{b}^p = \overline{c}^p = \overline{d}^p = 1, [\overline{a}, \overline{b}] = \overline{c}, [\overline{c}, \overline{a}] = \overline{1}, [\overline{c}, \overline{b}] = \overline{d}\rangle,$$

与上面相同的论证可得, G 有 p^4 阶交换子群. □

引理 11.8.12 设 G 是 $\mathcal{N}_{p^2}$ 群, N 是 G 的极大阶的交换正规子群. 若 $|N| = p^5$, 则 $N \cong \mathrm{C}_{p^3} \times \mathrm{C}_{p^2}$ 或 $\mathrm{C}_{p^2} \times \mathrm{C}_{p^2} \times \mathrm{C}_p$.

证明 由引理 11.8.6 可知 N 不循环且 $r(G) \leqslant 3$. 故 N 同构于

$$\mathrm{C}_{p^4} \times \mathrm{C}_p, \quad \mathrm{C}_{p^3} \times \mathrm{C}_{p^2}, \quad \mathrm{C}_{p^3} \times \mathrm{C}_p \times \mathrm{C}_p \quad 或 \quad \mathrm{C}_{p^2} \times \mathrm{C}_{p^2} \times \mathrm{C}_p.$$

令 $g_1 \in G \setminus N$ 使得 g_1 在 N 上诱导一个 p 阶自同构且 $K_1 = \langle N, g_1\rangle$. 下证 N 不同构于 $\mathrm{C}_{p^4} \times \mathrm{C}_p$ 和 $N \cong \mathrm{C}_{p^3} \times \mathrm{C}_p \times \mathrm{C}_p$.

若 $N = \langle a\rangle \times \langle b\rangle \cong \mathrm{C}_{p^4} \times \mathrm{C}_p$, 则 $o(g_1) \leqslant p^5$. 由引理 11.8.8 可得, $c(K_1) = 2$, $\langle a^p\rangle \times \langle b\rangle < C_G(g_1)$ 且 K_1 是 p 交换的. 于是当 $o(g_1) \leqslant p^2$ 时, $\langle g_1\rangle \trianglelefteq G$.

若 $o(g_1) = p$, 则 $[N, \langle g_1\rangle] = 1$. 这与 g_1g_1 在 N 上诱导一个 p 阶自同构矛盾. 若 $o(g_1) = p^2$, 则存在 s 和 t 使得 $g_1^p = a^{sp^3}b^t$. 若 $p \mid t$, 则 $g_1^p = a^{sp^3}$. 令 $g_2 = g_1a^{-sp^2}$. 则 $o(g_2) = p$, $K_1 = \langle N, g_2\rangle$ 且 g_2 在 N 上诱导一个 p 阶自同构, 这也是矛盾. 设 $p \nmid t$. 则 $N = \langle a\rangle \times \langle g_1^p\rangle$. 注意到 $[a, g_1] = g_1^{jp} \neq 1$. 则 $\langle a^{p^2}g_1\rangle \ntrianglelefteq G$. 另一方面, 因为 $\langle a^p\rangle \times \langle g_1\rangle \leqslant N_G(\langle a^{p^2}g_1\rangle)$, 故 $|N_G(\langle a^{p^2}g_1\rangle)| \geqslant p^3 o(a^{p^2}g_1)$. 从而 $\langle a^{p^2}g_1\rangle \trianglelefteq G$, 矛

盾. 于是 $o(g_1) \geqslant p^3$. 若 $o(g_1) = p^3$ 或 p^4, 则存在 s_1 和 t_1 使得 $g_1^p = a^{s_1p}b^{t_1}$. 现在有 $g_1^{p^2} = a^{s_1p^2}$. 令 $g_2 = g_1a^{-s_1}$. 则 $o(g_2) = p^2$ 且 g_2 在 N 上诱导一个 p 阶自同构, 这也是矛盾. 若 $o(g_1) = p^5$, 存在 s_3 使得 $(s_3, p) = 1$ 且 $g_1^p = a^{s_3}b^{t_3}$. 故可设 $N = \langle g_1^p\rangle \times \langle b\rangle$. 由引理 11.8.8 可知, $b \in Z(G)$ 且 g_1 在 N 上诱导恒等自同构. 这与假设矛盾. 同理可证, $N \ncong C_{p^3} \times C_p \times C_p$. □

引理 11.8.13 设 G 是 $\mathcal{N}_{p^2}$ 群, N 是 G 的极大阶的交换正规子群. 若 $|G| \geqslant p^6$, 则 $\mho_1(G) \leqslant N$ 且 $|N| = p^5$.

证明 见 [281]. □

定理 11.8.14 设 G 是 $\mathcal{N}_{p^2}$. 则 $|G| \leqslant p^6$. 若 $|G| = p^6$, 则 G 是下列互不同构的群之一.

(1) $G = \langle a, b \mid a^{p^3} = b^{p^3} = 1, [a, b] = a^{p^2}\rangle$;

(2) $G = \langle a, b, c \mid a^{p^2} = b^{p^2} = c^{p^2} = 1, [a, b] = 1, [a, c] = a^p, [b, c] = b^p\rangle$.

证明 设 $|G| \geqslant p^6$ 且 N 是 G 的极大阶的交换正规子群. 由引理 11.8.12 和引理 11.8.13 可知, $N \cong C_{p^3} \times C_{p^2}$ 或 $C_{p^2} \times C_{p^2} \times C_p$. 令 $g \in G \setminus N$ 使得 g 在 N 上诱导一个 p 阶自同构且 $K = \langle N, g\rangle$. 则 K 是 p 交换的. 由引理 11.8.8 推出 $o(g) \geqslant p^2$, 即对任意的 $g \in G \setminus N$ 有 $o(g) \geqslant p^2$. 分 $N \cong C_{p^3} \times C_{p^2}$ 和 $N \cong C_{p^2} \times C_{p^2} \times C_p$ 两种情形讨论. 我们断言 $K = G$.

情形 1 $N = \langle a\rangle \times \langle b\rangle \cong C_{p^3} \times C_{p^2}$. 此时 $\langle b\rangle \trianglelefteq G$, $\langle a^p\rangle \trianglelefteq G$ 且 $o(g) \leqslant p^4$.

首先证明 $o(g) = p^3$: 若 $o(g) = p^4$, 所以 $N = \langle g^p\rangle \times \langle b\rangle$. 因为 $b \notin C_G(g)$, 故 g 在 $\langle b\rangle$ 诱导一个 p 阶自同构. 于是存在 l_1 使得 $(l_1, p) = 1$ 且 $(g^{p^2}b)^g = g^{p^2}b^{1+l_1p}$. 注意到 $\langle g^{p^2}b\rangle \trianglelefteq G$. 故存在 τ 使得 $(g^{p^2}b)^g = (g^{p^2}b)^\tau$. 由此可得 $1 \equiv \tau \equiv 1 + l_1p (\mathrm{mod}\ p^2)$. 从而 $p | l_1$. 与 $(l_1, p) = 1$ 矛盾. 若 $o(g) = p^2$, 可设 $g^p = a^{sp^2}b^{tp}$. 令 $g_1 = ga^{-sp}b^{-t}$. 则 $o(g_1)$=p. 显然, $g_1 \in G \setminus N$, 这与当 $g \in G \setminus N$ 时, $o(g) \geqslant p^2$ 矛盾. 故 $o(g) = p^3$.

设 $g^p = a^{s_1p}b^{t_1}$. 若 $p | t_1$, 则 $o(ga^{-s_1}b^{-t_1'}) = p$, 其中 $t_1 = t_1'p$. 令 $g_1 = ga^{-s_1}b^{-t_1'}$. 则 $g_1 \in G \setminus N$ 且 $o(g_1) = p$, 矛盾. 故 $p \nmid t_1$. 于是 $N = \langle a\rangle \times \langle g^p\rangle$. 从而 $K = \langle a, g \mid a^{p^3} = g^{p^3} = 1, [a, g] = a^{k'p^2}g^{j'p^2}\rangle$. 计算可知,

$$K \cong K^1 = \langle a_1, b_1 \mid a_1^{p^3} = b_1^{p^3} = 1, [a_1, b_1] = a_1^{p^2}\rangle.$$

再证 G 同构于群 (1): 设 $K < G$. 则存在 $M \leqslant G$ 使得 $K \lessdot M \leqslant G$ 且 $g_2 \in M \setminus K$. 容易看出, g_2 在 N 上诱导一个 p 阶自同构. 与上面的论证类似可知, $o(g_2) = p^3$. 因为 g_2 在 K 上诱导一个 p 阶自同构且 $\langle g^p\rangle \trianglelefteq G$, 不妨设 $g^{g_2} = g^{1+i_1p^2}a^{j_1p^2}$. 由此得 $c(M) = 2$ 且 $\exp(M') = p$. 故 M 是 p 交换的. 注意到 $N = \langle a\rangle \times \langle g^p\rangle$. 则 $g_2^p = a^{s_2p}g^{t_2p}$. 令 $g_3 = g_2a^{-s_2}g^{-t_2}$. 则 $o(g_3) = p$. 显然, $g_3 \in G \setminus N$. 矛盾. 因而 $G = K \cong K^1$. 此为群 (1).

情形 2　$N=\langle a\rangle\times\langle b\rangle\times\langle c\rangle\cong \mathrm{C}_{p^2}\times\mathrm{C}_{p^2}\times\mathrm{C}_p$. 此时 $\langle a\rangle,\langle b\rangle,\langle c\rangle\trianglelefteq G$ 且 $o(g)\leqslant p^3$.

首先证明 $o(g)=p^2$: 若 $o(g)=p^3$, 则 $N=\langle g^p\rangle\times\langle b\rangle\times\langle c\rangle$. 因为 $b\notin C_G(g)$, 所以 g 在 $\langle b\rangle$ 上诱导一个 p 阶自同构. 故存在 l_1 使得 $(l_1,p)=1$ 且 $(g^pb)^g=g^pb^{1+l_1p}$. 注意到 $\langle g^pb\rangle\trianglelefteq G$. 则存在 t 使得 $(g^pb)^g=(g^pb)^t$. 由此可得 $1\equiv t\equiv 1+l_1p \pmod{p^2}$, 从而 $p|l_1$. 矛盾. 故 $o(g)=p^2$.

设 $g^p=a^{sp}b^{tp}c^l$. 若 $p|l$, 则 $(ga^{-s}b^{-t})^p=1$. 令 $g_1=ga^{-s}b^{-t}$. 则 $o(g_1)=p$ 且 $g_1\in G\setminus N$, 矛盾. 故 $p\nmid l$. 不妨设 $N=\langle a\rangle\times\langle b\rangle\times\langle g^p\rangle$. 若 $[a,g]=1$, 则 $\langle g\rangle\trianglelefteq G$. 从而 $[b,g]=1$. 这与 g 在 N 上诱导 p 阶自同构矛盾. 故

$$K=\langle a,b,g\mid a^{p^2}=b^{p^2}=g^{p^2}=1,[a,g]=a^p,[b,g]=b^{np}\rangle,\quad 1\leqslant n\leqslant p-1.$$

若 $n\geqslant 2$, 则 $\langle ab\rangle\ntrianglelefteq G$. 然而, $\langle a,b,g^p\rangle\leqslant N_G(\langle ab\rangle)$ 且 $|\langle a,b,g^p\rangle|=p^3o(ab)$, 矛盾. 因而 $n=1$.

再证 G 同构于群 (2): 设 $K<G$. 则存在 $M\leqslant G$ 使得 $K\lessdot M\leqslant G$ 且 $g_2\in M\setminus K$. 与上面论证类似可得, g_2 在 N 上诱导 p 阶自同构且 $o(g_2)=p^2$. 注意到 $N=\langle a\rangle\times\langle b\rangle\times\langle g^p\rangle$. 则 $g_2^p=a^{s_1p}b^{t_1p}g^{l_1p}$. 令 $g_3=g_2a^{-s_1}b^{-t_1}g^{-l_1}$. 则 $o(g_3)=p$. 显然, $g_3\in G\setminus N$, 矛盾. 因而 $G=K$. 此为群 (2).

反之易证定理中的两类群互不同构且是 $\mathcal{N}_{p^2}$ 群. □

若 G 是 p^5 阶的 $\mathcal{N}_{p^2}$ 群, 使用 [270] 给出的 p^5 阶群的分类及使用 Magma 检查小群库中的群, 文献 [281] 列出了结果.

11.8.3　非正规子群在其正规化子中的指数为 $p^i(i\geqslant 3)$ 的 p 群

本节分类 $\mathcal{S}_i$ 群, 即非正规子群在其正规化子中的指数恰为 p^i 的有限 p 群. 这里 $i\geqslant 3$. 本节内容取自 [277].

定理 11.8.15　*设 G 是非 Dedekind p 群, i 是大于 2 的整数. 则 $G\in\mathcal{S}_i$ 当且仅当 G 是下列互不同构的群之一.*

(1) $\mathrm{M}_p(i+1,m)$, $m\leqslant i+1$;

(2) $\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^i}$;

(3) $\mathrm{D}_8*\mathrm{Q}_8(i=3)$;

(4) $\langle a,b,c,d\mid a^4=b^4=c^4=d^4=1,a^2=d^2,b^2=c^2,[d,b]=a^2,[b,a]=a^2,[c,a]=b^2,[d,a]=[c,b]=a^2b^2,[c,d]=1\rangle(i=3)$.

证明　$\Longrightarrow$: 分两种情形讨论.

情形 1　$|G'|=p$.

设 N_1 是 G 的极小阶的非正规子群. 则 N_1 的所有极大子群在 G 中正规. 于是 N_1 不能由它的极大子群生成. 由此可得 N_1 有唯一的极大子群. 于是 N_1 循环.

令 $N_1=\langle b\rangle$. 因为 $N_1 \ntrianglelefteq G$, 故存在 $a\in G$ 使得 $[a,b]\neq 1$. 因为 $|G'|=p$, 故 $\langle a,b\rangle$ 是 G 的内交换子群. 令 $H=\langle a,b\rangle$. 由引理 10.1.1 可得, $G=H*C_G(H)$. 因为 H 内交换, 故 $C_H(N_1)\lessdot H$. 从而 $C_G(N_1)\geqslant C_G(H)$ 且 $C_G(N_1)\geqslant C_H(N_1)$. 于是 $C_G(N_1)=N_G(N_1)\lessdot G$. 由 $G\in\mathcal{S}_3$ 可知, N_1 是 G 的具有极大阶的非正规子群. 由此推出 G 的所有非正规子群有相同的阶.

若 G 的所有非正规子群均为 p 阶, 由定理 11.1.7 可知, G 是下列群之一

$$\mathrm{M}_p(i+1,1),\quad \mathrm{M}_p(1,1,1)*\mathrm{C}_{p^i}\quad 或\quad \mathrm{D}_8*\mathrm{Q}_8\quad (i=3).$$

若 G 的所有非正规子群均为 p^m 阶, 其中 $m\geqslant 2$, 则 $\Omega_1(G)\leqslant Z(G)$. 若 $p>2$, 由 [181] 中的引理 3.2 可知, $G\cong \mathrm{M}_p(i+1,m)$, 其中 $m\leqslant i+1$. 若 $p=2$, 因为 $G=H*C_G(H)$, 故 $G\in\mathcal{S}_i$, 从而 $H\in\mathcal{S}_i$. 由此可得 $H\cong\mathrm{M}_2(i+1,m)$, 其中 $m\leqslant i+1$. 设 $C_G(H)\nleqslant H$. 则存在 $c\in C_G(H)\backslash H$. 令 $H=\langle a\rangle\rtimes\langle b\rangle$ 且 $c^{2^n}=a^{2^s}b^{2^t}$, $n,s,t\geqslant 1$. 矛盾. 于是 $C_G(H)\leqslant H$, $G\cong\mathrm{M}_2(i+1,m)$, 其中 $m\leqslant i+1$.

若 $s\geqslant 2$, 则 $c_1=c^{-2^{n-1}}a^{2^{s-1}}b^{2^{t-1}}\notin H$ 且有阶 p. 于是 $\langle b,c_1\rangle\ntrianglelefteq G$ 且 $|\langle b,c_1\rangle|\neq|\langle b\rangle|$. 这与 G 的所有非正规子群同阶矛盾.

若 $s=1$ 且 $t\geqslant 2$, 则 $c_1=c^{-2^{n-1}}ab^{2^{t-1}}\notin H$ 且有阶 p. 于是 $\langle c_1\rangle\ntrianglelefteq G$ 且 $|\langle c_1\rangle|\neq|\langle b\rangle|$. 这又与 G 的所有非正规子群同阶矛盾.

若 $s=1$ 且 $t=1$, 令

$$K=\langle H,c\rangle=\langle a,b,c\mid a^{2^{i+1}}=b^{2^m}=1,[a,b]=a^{2^i},c^{2^n}=a^2b^2,[c,a]=[c,b]=1\rangle,$$

其中 $m\leqslant i+1$. 若 $i+1\geqslant 3$, 则 $c_1=c^{-2^{n-1}}aba^{2^i}\notin H$ 且有阶 p. 于是 $\langle c_1\rangle\ntrianglelefteq G$ 且 $|\langle c_1\rangle|\neq|\langle b\rangle|$. 这与 G 的所有非正规子群具有阶 $|N_1|$ 矛盾. 若 $i+1=m=2$, 因为 $G\in\mathcal{S}_3$ 且 $\langle b\rangle\ntrianglelefteq G$, 故 $n\geqslant 2$. 于是 $\langle ca\rangle\ntrianglelefteq G$, 且 $|\langle ca\rangle|\neq|\langle b\rangle|$. 这还是与 G 的所有非正规子群同阶矛盾.

情形 2 $|G'|\geqslant p^2$.

对 $|G|$ 作归纳. 若 $|G|=p^5$ 且 $G\in\mathcal{S}_3$, 则 G 的所有非正规子群均为 p 阶. 由定理 11.1.7 可知, G 是下列群之一: $G\cong\mathrm{M}_p(4,1)$, $\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^3}$ 或 $\mathrm{D}_8*\mathrm{Q}_8$. 结论成立. 设结论对阶 $<|G|$ 的群成立. 因为 G 是 p 群, 存在 p 子群 N 使得 $N\leqslant G'\bigcap Z(G)$. 由引理 11.8.1 及归纳假设得, G/N 是定理中的群之一.

当 G/N 同构于定理中的群 (1), (2), (4) 时, 将导出矛盾. 当 G/N 同构于 (3) 时, 则可得 G 同构于群 (4). 因而定理的结论成立. 证明细节略去.

$\Longleftarrow$: 由 [181] 中的引理 3.2 及定理 11.1.7 可知, 群 (1)—(3) 是 $\mathcal{S}_i$ 群. 若 G 同构于群 (4), 则 $G'=\langle a^2\rangle\times\langle b^2\rangle=Z(G)=\Omega_1(G)$. 易证 G 的所有 2^5 阶的商群同构于 $\mathrm{Q}_8*\mathrm{D}_8$. 设 $H\ntrianglelefteq G$. 下证 $|N_G(H):H|=2^3$. 于是 $G\in\mathcal{S}_3$.

若 $|H|=2^4$, 则 $|H\bigcap\Omega_1(G)|=2$. 令 $\overline{G}=G/H\bigcap\Omega_1(G)$. 因为 $|\overline{G}|=2^5$, 故 $\overline{G}$ 同构于群 (3). 但是 $|\overline{H}|=2^3$. 由定理 11.1.7 可知 $\overline{H}\trianglelefteq\overline{G}$. 故 $H\trianglelefteq G$, 矛盾.

若 $|H|=2^3$, 则 $|H\bigcap\Omega_1(G)|=2$. 令 $\overline{G}=G/H\bigcap\Omega_1(G)$. 因为 $|\overline{G}|=2^5$, $\overline{G}$ 同构于群 (3). 但是 $|\overline{H}|=2^2$. 仍由定理 11.1.7 可得 $\overline{H}\trianglelefteq\overline{G}$. 故 $H\trianglelefteq G$, 矛盾.

若 $|H|=2^2$, 则 $|H\bigcap\Omega_1(G)|=2$. 令 $\overline{G}=G/H\bigcap\Omega_1(G)$. 因为 $|\overline{G}|=2^5$, 故 $\overline{G}$ 同构于群 (3). 然而 $|\overline{H}|=2$. 由 $H\ntrianglelefteq G$ 推出 $\overline{H}\ntrianglelefteq\overline{G}$. 再由定理 11.1.7 可得 $|N_{\overline{G}}(\overline{H}):\overline{H}|=2^3$. 于是 $|N_G(H):H|=|N_{\overline{G}}(\overline{H}):\overline{H}|=2^3$.

若 $|H|=2$, 因为 $\Omega_1(G)=\langle a^2\rangle\times\langle b^2\rangle=Z(G)$, 故 $H\trianglelefteq G$, 矛盾. □

11.8.4 非正规子群在其正规化子中的商群循环的 p 群

设 G 为有限 p 群. 若对 G 的所有非正规子群 H 均有 $N_G(H)/H$ 循环, 则称 G 为 $\mathcal{N}_c$ 群. 张军强在文献 [262] 分类了 $\mathcal{N}_c$ 群. 本节介绍该分类结果.

引理 11.8.16 设 G 是 $\mathcal{N}_c$ 群. 则下列结论成立.

(1) 若 $H\leqslant G$, 则 H 也是 $\mathcal{N}_c$ 群;

(2) 若 $N\trianglelefteq G$, 则 G/N 也是 $\mathcal{N}_c$ 群;

(3) 若 G 不是 Dedekind p 群, 则 G 没有 p^3 阶初等交换子群.

证明 (1) 设 L 是 H 的非正规子群. 则 L 在 G 中非正规且 L 是 H 的真子群. 因为 G 是 $\mathcal{N}_c$ 群, 故 $N_G(L)/L$ 循环. 于是 $N_H(L)/L$ 也循环.

(2) 设 T/N 是 G/N 的非正规子群. 则 T 在 G 中非正规. 因为 G 是 $\mathcal{N}_c$ 群, 故 $N_G(T)/T$ 循环. 于是 $(N_G(T)/N)/(T/N)$ 也循环. 任取 $gN\in N_{G/N}(T/N)$, 则 $(T/N)^g=T/N$ 且 $T^g=T$. 因此 $N_{G/N}(T/N)=N_G(T)/N$. 从而

$$N_{G/N}(T/N)/(T/N)=(N_G(T)/N)/(T/N)$$

也循环.

(3) 若否, 设 L 是 G 的 p^3 阶初等交换子群. 则对 L 的任意 p 阶子群 K 有 $N_G(K)/K\geqslant L/K$ 非循环. 于是 $K\trianglelefteq G$. 从而 $L\leqslant Z(G)$. 设 H 是 G 的极小阶非正规子群. 由引理 11.1.1 可得, H 循环. 于是 $|H\bigcap L|\leqslant p$. 从而 $N_G(H)/H\geqslant HL/H\cong L/L\bigcap H$, 非循环, 矛盾. 故 G 没有 p^3 阶初等交换子群. □

下面我们分类 $\mathcal{N}_c$ 群. 分 $|G'|=p$, $|G'|=p^2$ 和 $|G'|\geqslant p^3$ 三种情形讨论.

定理 11.8.17 设 G 是有限 p 群, $|G'|=p$. 则 G 是 $\mathcal{N}_c$ 群当且仅当 G 为下列互不同构的群之一.

(1) Hamilton p 群;

(2) $\mathrm{M}_p(n,m)=\langle a,b\mid a^{p^n}=b^{p^m}=1,[a,b]=a^{p^{n-1}}\rangle$, 其中 $n\geqslant 2$;

(3) $\mathrm{Q}_8\times\mathrm{C}_{2^{k+1}}=\langle a,b,c\mid a^4=1,b^2=a^2,[a,b]=a^2,c^{2^{k+1}}=1,[a,c]=[b,c]=1\rangle$, 其中 $k\geqslant 1$, $\Omega_1(G)=\langle a^2,c^2\rangle\cong\mathrm{E}_{2^2}$;

(4) $\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^{k+1}}=\langle a,b,c \mid a^p=b^p=c^{p^{k+1}}=1,[a,b]=c^{p^k},[c,a]=[c,b]=1\rangle$, 其中 $k\geqslant 1$, 如果 $p=2$, $\Omega_1(G)=\langle a,b,c^{p^k}\rangle\cong \mathrm{M}_p(1,1,1)$.

证明 使用导群 p 阶的有限 p 群的结构定理, 见定理 10.1.2, 结论不难得到. 证明略去. □

定理 11.8.18 设 G 是有限 p 群, $|G'|=p^2$. 则 G 是 $\mathcal{N}_c$ 群当且仅当 G 为下列互不同构的群之一.

(1) $\langle a,b,c \mid a^4=c^4=1,b^2=a^2,[a,b]=a^2c^2,[a,c]=c^2,[b,c]=1\rangle$, 此时 G 是 2^5 阶内亚循环群, $\Omega(G)=\langle a^2,c^2\rangle\cong \mathrm{E}_{2^2}$;

(2) $\langle a,b,c \mid a^p=b^{p^2}=c^p=1,[a,b]=c,[a,c]=b^{vp},[b,c]=1\rangle$, 其中 $p>2$ 且 $v=1$ 或者是一个固定的模 p 的平方非剩余, $\Omega(G)=\langle a,c,b^p\rangle\cong \mathrm{M}_p(1,1,1)$;

(3) $\langle a,b,c \mid a^{3^3}=c^3=1,b^3=a^{-3},[a,b]=c,[a,c]=a^3,[b,c]=1\rangle$, 此时 G 是 3^4 阶极大类的内亚循环群, $\Omega(G)=\langle a^3,c\rangle\cong \mathrm{E}_{2^2}$;

(4) 2^4 阶极大类 2 群;

(5) $\langle a,b \mid a^{2^n}=b^{2^m}=1,[a,b]=a^{-2+t2^{n-1}}\rangle, n=3, t\in\{0,1\}, m\in\{2,3\}$;

(6) $\langle a,b \mid a^{2^n}=1,b^4=a^{2^{n-1}},[a,b]=a^{-2}\rangle, n=3$.

证明 设 G 是一个 $|G'|=p^2$ 的 $\mathcal{N}_c$ 群. 则存在 $N\leqslant G'$ 使得 N 是 G 的 p 阶正规子群. 令 $\overline{G}=G/N$. 则由引理 11.8.16 可得, $\overline{G}$ 是导群 p 阶的 $\mathcal{N}_c$ 群. 从而 $\overline{G}$ 同构于定理 11.8.17 中的群之一. 对 $\overline{G}$ 的各种情形讨论即可得结论. 证明略去. □

定理 11.8.19 设 G 是有限 p 群, $|G'|\geqslant p^3$. 则 G 是 $\mathcal{N}_c$ 群当且仅当 G 同构于下列的群之一.

(1) 阶 $\geqslant 2^5$ 的极大类 2 群;

(2) $\langle a,b \mid a^{2^n}=b^{2^m}=1,[a,b]=a^{-2+t2^{n-1}}\rangle$, 其中 $n\geqslant 4, t\in\{0,1\}, m\in\{2,3\}$;

(3) $\langle a,b \mid a^{2^n}=1,b^4=a^{2^{n-1}},[a,b]=a^{-2}\rangle$, 其中 $n\geqslant 4$.

证明 假设 G 是 $|G'|=p^3$ 的 $\mathcal{N}_c$ 群. 则存在 G 的 p 阶正规子群 $N\leqslant G'\bigcap Z(G)$. 由引理 11.8.16 可得, $\overline{G}=G/N$ 是 $\mathcal{N}_c$ 群. 于是 $\overline{G}$ 是 $|G'|=p^2$ 的 $\mathcal{N}_c$ 群. 从而 $\overline{G}$ 同构于定理 11.8.18 的群之一. 对 $\overline{G}$ 的各种情形讨论及使用归纳法即可得结论. 证明略去. □

设 G 是有限 p 群. 注意到 $p>2$ 时, 子群 H 是 1-单列的当且仅当 $N_G(H)/H$ 循环. 于是由 $\mathcal{N}_c$ 群的分类定理即得如下推论.

推论 11.8.20 设 G 是有限 p 群, $p>2$. 则 G 的非正规子群均是 1-单列的当且仅当 G 同构于下列互不同构的群之一.

(1) 交换 p 群;

(2) $\mathrm{M}_p(n,m)=\langle a,b \mid a^{p^n}=b^{p^m}=1,[a,b]=a^{p^{n-1}}\rangle$, $n\geqslant 2$;

(3) $\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^{k+1}}=\langle a,b,c \mid a^p=b^p=c^{p^{k+1}}=1,[a,b]=c^{p^k},[c,a]=[c,b]=1\rangle$, 若 $p=2$ 时, $k\geqslant 1$, $\Omega_1(G)=\langle a,b,c^{p^k}\rangle\cong \mathrm{M}_p(1,1,1)$;

(4) $\langle a,b,c \mid a^p=b^{p^2}=c^p=1,[a,b]=c,[a,c]=b^{vp},[b,c]=1\rangle$, $v=1$ 或是一个固定的模 p 的平方非剩余;

(5) $\langle a,b,c \mid a^{3^3}=c^3=1,b^3=a^{-3},[a,b]=c,[a,c]=a^3,[b,c]=1\rangle$, 此时 G 是一个 3^4 阶极大类的内亚循环群.

定理 11.8.21 设 G 是有限 p 群. 则 G 的非正规子群均单列嵌入于 G 当且仅当 G 同构于下列互不同构的群之一.

(1) Hamilton p 群;

(2) $\mathrm{M}_p(n,m)=\langle a,b \mid a^{p^n}=b^{p^m}=1,[a,b]=a^{p^{n-1}}\rangle$, $n\geqslant 2$;

(3) $\mathrm{M}_p(1,1,1)$, $p>2$;

(4) 阶 $\geqslant 2^4$ 的极大类 2 群;

(5) $\langle a,b \mid a^{2^n}=b^{2^2}=1,[a,b]=a^{-2+t2^{n-1}}\rangle, n\geqslant 3, t\in\{0,1\}$.

证明 设 G 不是 Hamilton p 群. 若 G 为 (2) 型群, 则 G 为亚循环的内交换 p 群且 $\Phi(G)=Z(G)$. 从而 G 的非正规子群 H 都包含 G 的一个生成元且 $\langle H,\Phi(G)\rangle=C_G(H)$ 是 G 的包含 H 的唯一的极大子群. 因为 $C_G(H)/H=N_G(H)/H$ 循环, 故 H 单列嵌入于 $C_G(H)$. 于是 H 单列嵌入于 G. 若 G 是 (3) 型群, 则 $d(G)=2$ 且 $|G|=p^3$. 从而 G 的非正规子群 H 都为 p 阶且包含于唯一的 p^2 阶子群 $\langle H,\Phi(G)\rangle$ 中. 故 H 单列嵌入于 $C_G(H)$. 于是 H 单列嵌入于 G. 若 G 为 (4) 型群, 则 G 是 $\mathcal{S}_1$ 群. 于是

$$G=\langle a,b \mid a^{2^{n+1}}=1,b^2=a^{i2^n},[a,b]=a^{-2+t2^n}\rangle,$$

其中 $i,t\in\{0,1\}$. 则 $\Phi(G)=\langle a^2\rangle$ 且其所有子群都正规于 G. 从而 H 非正规当且仅当 $H=\langle a^{2^x},ba^i\rangle$, 其中 $x\geqslant 2$ 包含 H 的极大链为

$$H=\langle a^{2^x},ba^i\rangle \lessdot \langle a^{2^{x-1}},ba^i\rangle \lessdot \cdots \lessdot \langle a^2,ba^i\rangle \lessdot G,$$

这个链是唯一的. 于是 H 单列嵌入于 G. 若 G 为 (5) 型群, 则 G 是 $\mathcal{S}_1$ 群, $\Phi(G)=\langle a^2,b^2\rangle$ 且其所有子群都正规于 G. 类似可得, G 的非正规子群都单列嵌入于 G.

反之, 若 G 的非正规子群都单列嵌入于 G, 则 G 是 $\mathcal{N}_c$ 群. 验证易得, G 为定理中所列的群之一. □

注 11.8.22 Blackburn 等在文献 [34] 研究了 n 单列性何时可以推出单列嵌入的问题. 他们证明了: 对 $p>3$, 2-单列循环子群一定是单列嵌入的. 然而, 1-单列循环子群不一定是单列嵌入的. 例如, 在推论 11.8.20 中, $k\geqslant 1$ 的 (3) 型群、(4) 型群和 (5) 型群都有 1-单列循环子群但它们不是单列嵌入的.

11.9 非正规子群生成真子群的 p 群

Cappitt[45] 从非正规子群生成真子群的角度研究比 Dedekind 群更大的群类. 设 G 是有限群. Cappitt 在文献 [45] 引进了一个新的子群概念: $S(G)=\langle H\leqslant G\mid H\ntrianglelefteq G\rangle$. 显然, 一个 Dedekind 群 G 恰是 $S(G)=1$ 的群. Cappitt 称 $S(G)<G$ 的群 G 为广义 Dedekind 群. 他证明了: 广义 Dedekind 群的幂零类至多是 2. Reboli 和 Kappe 在文献 [110], [191] 对广义 Dedekind 群做了进一步研究. 她们证明了: 广义 Dedekind 群的导群是循环的, 且分类了二元生成的广义 Dedekind 群. Reboli 在文献 [191] 引进了又一个子群概念: $CS(G)=\langle g\in G\mid\langle g\rangle\ntrianglelefteq G\rangle$. 她证明了: 对于任意群 G, 均有 $CS(G)=S(G)$. 曲海鹏在文献 [189] 给出了 Dedekind 群和广义 Dedekind 群的一个新刻画. 本节介绍他的结果.

显而易见, 有限群 G 是 Dedekind 群当且仅当对每个 $x\in G$ 都有 $\langle x\rangle\trianglelefteq G$. 进一步地, 我们还有下列刻画.

定理 11.9.1 *设 G 为有限群. 若对 $x\in G\setminus\Phi(G)$ 均有 $\langle x\rangle\trianglelefteq G$, 则 G 为 Dedekind 群.*

证明 由于 $G/\Phi(G)$ 为 Dedekind 群, 因此 G 幂零. 假设 G 为极小阶反例. 则 G 为 p 群. 进而, 由引理 11.1.2 知, 存在 $N\trianglelefteq G$ 且 $N\lessdot G'$ 使得 G/N 非 Dedekind 群. 因而 $|G'|=p$. 从而 $\Phi(G)=G'\mho_1(G)\leqslant Z(G)$. 因此任取 $x\in G$, $\langle x\rangle\trianglelefteq G$, 即 G 为 Dedekind 群, 矛盾. □

为方便, 有限群 G 称为 $\mathcal{P}$ 群, 若 G 有一个极大子群 M 使得对任意的 $x\in G\setminus M$ 都有 $\langle x\rangle\trianglelefteq G$. 下面我们给出广义 Dedekind 群的若干性质并证明: G 是广义 Dedekind 群当且仅当 G 是 $\mathcal{P}$ 群.

引理 11.9.2 *设 G 为有限群, $M\lessdot G$ 且 $M\trianglelefteq G$. 则 $G'=[G\setminus M,M]$.*

证明 令 $N=[G\setminus M,M]$, $\overline{G}=G/N$ 且 $\overline{M}=M/N$. 显然只需证明 $\overline{G}$ 交换. 因为 $\overline{G}\setminus\overline{M}=\overline{G\setminus M}\subseteq C_{\overline{G}}(\overline{M})$, 所以 $|C_{\overline{G}}(\overline{M})|\geqslant 1+|\overline{G}\setminus\overline{M}|\geqslant 1+|\overline{G}|/2$. 因此 $C_{\overline{G}}(\overline{M})=\overline{G}$. 由于 $\overline{M}\lessdot\overline{G}$, 因此 $\overline{G}$ 交换. □

引理 11.9.3 *设 G 是 $\mathcal{P}$ 群. 则 G 幂零且 $c(G)\leqslant 2$.*

证明 任取 $x\in G\setminus M$, 则 $\langle x\rangle\trianglelefteq G$. 因此 $G/C_G(x)\lesssim\mathrm{Aut}(\langle x\rangle)$. 注意到循环群的自同构群交换, 因此 $G'\leqslant C_G(x)$. 从而 $G'\leqslant C_G(G\setminus M)=C_G(G)=Z(G)$. □

下面, 我们总假设 G 为有限 p 群.

定理 11.9.4 *设 G 是 $\mathcal{P}$ 群. 则 G' 循环.*

证明 选取适当的 $a\in G\setminus M$ 使得 $[a,G]$ 极大. 因为 $[a,G]\leqslant\langle a\rangle\trianglelefteq G$, 所以 $[a,G]\trianglelefteq G$. 断言 $\overline{G}=G/[a,G]$ 交换. 因此 $G'=[a,G]$ 循环. 令 $H=\{x|\langle[a,x]\rangle<[a,G]\}$. 由于 $[a,G]$ 循环, 因此 $H<G$. 注意到 $a\in H\setminus M$, 因此 $G=\langle G\setminus(M\bigcup H),a\rangle$.

任取 $y \in G\backslash(M \bigcup H)$, 则 $[a,G] = \langle [a,y] \rangle \leqslant [y,G]$. 根据 a 的选取可知, $[y,G] = [a,G]$. 故 $\overline{G}$ 交换. □

引理 11.9.5 设 G 是有限群, G' 循环且 $M < G$. 若 $\langle [a,b] \rangle = G'$, 则存在 $x \in G \setminus M$ 使得 $\langle [a,x] \rangle = G'$.

证明 若否, 令 $\overline{G} = G/\mho_1(G')$. 则 $C_{\overline{G}}(\bar{a}) \geqslant \langle \overline{G} \setminus \overline{M} \rangle = \overline{G}$. 因此 $[a,b] \in \mho_1(G')$, 矛盾. □

引理 11.9.6 设 G 是 $\mathcal{P}$ 群.

(1) 若 $x \in G \setminus M$ 且 $[x,M] = G'$, 则 $o(x) = \exp(G)$;

(2) 若 $|G'| = 2$ 且 $\exp(G) = 4$, 则 G 为 Dedekind 群.

证明 (1) 先证当 $|G'| = p$ 时结论成立. 令 x 为最小阶元, 其中 $x \in G \setminus M$ 且 $[x,M] = G'$. 断言 $\exp(G) = o(x)$. 若否, 以下将证明 $x \in Z(G)$, 进而得出矛盾.

首先, 断言 $\langle x \rangle \bigcap \langle y \rangle = 1$, 其中 $y \in G$ 且 $o(x) < o(y)$. 若否, 不妨设 $x^{p^{m-1}} = y^{p^{n-1}}$, 其中 $o(x) = p^m, o(y) = p^n$. 因为 $|G'| = p$ 且 $n > m$, 所以 $y^{p^{n-m}} \in Z(G)$. 因此 $(xy^{-p^{n-m}})^{p^{m-1}} = 1$ 且 $[xy^{-p^{n-m}}, M] = G'$, 这与 $o(x)$ 的极小性矛盾.

其次, 任取 $y \in G$, 断言 $[x,y] = 1$. 假设 $o(x) < o(y)$. 若 $y \in G \setminus M$, 则 $\langle y \rangle \trianglelefteq G$. 因此 $[x,y] \in \langle x \rangle \bigcap \langle y \rangle = 1$. 若 $y \in M$, 则 $xy \in G \setminus M$. 注意到 $o(y) > o(x) > |G'| = p$ 且 G 为 p^2 交换的, 则 $o(xy) = o(y)$. 从而 $[x,xy] = 1$. 进而 $[x,y] = 1$. 假设 $o(x) \geqslant o(y)$. 则可选取适当的 $z \in G$ 使得 $o(z) > o(x)$. 从而 $o(zy) = o(z)$. 因此 $[x,z] = [x,zy] = 1$. 故 $[x,y] = 1$. 也即当 $|G'| = p$ 时结论成立.

令 $\overline{G} = G/\mho_1(G')$. 根据定理 11.9.4 及上述所证可知, $o(\bar{x}) = \exp(\overline{G})$. 因为 $[x,M] = G'$, 所以 $G' \leqslant \langle x \rangle$. 因此

$$o(x) = o(\bar{x})|\mho_1(G')| = \exp(\overline{G})|\mho_1(G')| \geqslant \exp(G).$$

故 $o(x) = \exp(G)$.

(2) 若否, 则存在元素 $a \in M$ 使得 $\langle a \rangle \ntrianglelefteq G$. 由引理 11.9.5 知, 存在 $x \in G \setminus M$ 使得 $[a,x] \neq 1$. 令 $H = \langle a,x \rangle$. 容易验证 H 是 $\mathcal{P}$ 群. 因为 $\langle a \rangle \ntrianglelefteq G$ 且 $G' \leqslant \langle x \rangle$, 所以 $\langle a \rangle \bigcap \langle x \rangle = 1$. 从而 $H \cong \mathrm{M}_2(2,2)$ 或者 D_8. 因为 D_8 为 $\mathrm{M}_2(2,2)$ 的商群, 所以 D_8 是 $\mathcal{P}$ 群. 但容易验证 D_8 不是 $\mathcal{P}$ 群, 矛盾. □

引理 11.9.7 设 G 非 Dedekind 群且 $\exp(G) = p^e$. 若 G 是 $\mathcal{P}$ 群且 $|G'| = p$, 则 $M = \Omega_{e-1}(G)$.

证明 因为 $|G'| = p$, 所以当 $p > 2$ 时, G 是 p 交换的且当 $p = 2$ 时, G 是 4 交换的. 由引理 11.9.6(2) 知, 若 $p = 2$, 则 $\exp(G) \geqslant 8$. 因此 $\Omega_{e-1}(G) < G$.

下面来证明 $M \leqslant \Omega_{e-1}(G)$. 若否, 设 G 为一个极小阶反例. 则存在 $a \in M$ 且 $o(a) = p^e$. 由引理 11.9.2 知, 存在 $x \in G \setminus M$ 且 $[x,M] = G'$. 从而由引理 11.9.6(1) 知, $o(x) = p^e$.

若 $\langle[a,M]\rangle = G'$, 则由引理 11.9.5 知, 存在 $y \in G \setminus M$ 使得 $\langle[a,y]\rangle = G'$. 因为 G 为极小阶反例, 所以 $G = \langle a\rangle\langle y\rangle$ 且 $M = \langle a\rangle\langle y^p\rangle$. 我们断言 $\langle y\rangle \bigcap \langle a\rangle = 1$. 若否, 不失一般性, 可设 $y^{p^{e-1}} = a^{p^{e-1}}$. 因此 $(ya^{-1})^{p^{e-1}} = 1$. 因为 $\langle[ya^{-1},a]\rangle = \langle[y,a]\rangle = G'$, 所以由引理 11.9.6(1) 知 $o(ya^{-1}) = p^e$, 矛盾. 类似地可证, $\langle y\rangle \bigcap \langle ya\rangle = 1$. 因而 $[y,a] = [y,ya] \in \langle y\rangle \bigcap \langle ya\rangle = 1$, 矛盾.

若 $[a,M] < G'$, 则类似上面的证明可得 $\langle x\rangle \bigcap \langle a\rangle = 1$. 进而 $\langle x\rangle \bigcap \langle xa\rangle = 1$. 因为 $G' \leqslant \langle x\rangle$, 所以 $[xa,G] \in G' \bigcap \langle xa\rangle = 1$, 即 $xa \in Z(G)$. 因此 $[a,M] = [x,M] = G'$, 矛盾. □

定理 11.9.8 设 G 非 Dedekind 群且 $\exp(G) = p^e$. 若 G 是 $\mathcal{P}$ 群, 则 $M = \Omega_{e-1}(G)$.

证明 令 $\overline{G} = G/\mho_1(G')$. 假设 $|G'| = p^k$. 由引理 11.9.2、定理 11.9.4 以及引理 11.9.6(1) 知, $\exp(\overline{G}) = p^{e-k+1}$. 进而由引理 11.1.2 知, $\overline{G}$ 非 Dedekind. 根据引理 11.9.7 可知, $\overline{M} = \Omega_{e-k}(\overline{G})$. 因此 $M \leqslant \Omega_{e-1}(G)$. 由引理 11.9.6(2) 知, 若 $p=2$, 则 $e-k+1 \geqslant 3$. 因此 G 是 p^{e-1} 交换的且 $\Omega_{e-1}(G) < G$. 故 $M = \Omega_{e-1}(G)$. □

引理 11.9.9 设 G 非 Dedekind 群且 $\exp(G) = p^e$. 若 G 是 $\mathcal{P}$ 群且 $|G'| = p$, 则 $G' = \mho_{e-1}(G)$.

证明 由定理 11.9.8 知, G 为 p^{e-1} 交换的. 因此 $\mho_{e-1}(G) \cong G/\Omega_{e-1}(G) \cong \mathrm{C}_p$. 下面来证明 $G' \leqslant \mho_{e-1}(G)$. 事实上, 由引理 11.9.2 知, 存在 $x \in G\backslash M$ 且 $[x,M] = G'$. 由引理 11.9.6(2) 知, $o(x) = p^e$. 因此 $G' = \mho_{e-1}(\langle x\rangle) \leqslant \mho_{e-1}(G)$. □

定理 11.9.10 设 G 非 Dedekind 群且 $\exp(G) = p^e$. 若 G 是 $\mathcal{P}$ 群且 $|G'| = p^k$, $k \geqslant 1$, 则 $G' = \mho_{e-k}(G)$.

证明 由引理 11.9.2 知, 存在 $x \in G \setminus M$ 且 $[x,M] = G'$. 由引理 11.9.6(2) 知, $o(x) = p^e$. 令 $\overline{G} = G/\mho_1(G')$. 则 $\overline{G}$ 是 $\mathcal{P}$ 群. 进而, 由引理 11.1.2 知, G 非 Dedekind. 由引理 11.9.6(2) 知, $\exp(\overline{G}) = o(\bar{x})$. 由推论 11.9.9 知, $\mho_{e-k}(\overline{G}) = \overline{G}'$. 注意到 $\mho_{e-k}(\overline{G}) = \mho_{e-k}(G)/\mho_1(G')$. 因此 $\mho_{e-k}(G) = G'$. □

现在, 我们有如下的定理.

定理 11.9.11 设 G 是一个有限非 Dedekind p 群且 $\exp(G) = p^e$. 则 G 是 $\mathcal{P}$ 群当且仅当 $M = \Omega_{e-1}(G)$, $G' \cong \mathrm{C}_{p^k}$ 且 $\mho_{e-k}(G) = G'$.

证明 由定理 11.9.4、定理 11.9.8 以及定理 11.9.10 知, 我们只需证明充分性. 任取 $x \in G \setminus M$, 有 $o(x) = p^e$. 因此 $\mho_{e-k}(\langle x\rangle) = G'$. 因而 $\langle x\rangle \trianglelefteq G$. 故 G 是 $\mathcal{P}$ 群.□

根据这个定理, 我们可以给出有限广义 Dedekind 群是 $\mathcal{P}$ 群的一个新证明.

推论 11.9.12 有限群 G 是 $\mathcal{P}$ 群当且仅当 G 是广义 Dedekind 群.

证明 不失一般性, 假设 G 为有限非 Dedekind p 群. 下证若 G 是 $\mathcal{P}$ 群, 则 $S(G) \leqslant M$. 任取 $H \leqslant G$ 且 $H \nleqslant M$, 由定理 11.9.11 知, $\mho_{e-k}(H) = \mho_{e-k}(G) \geqslant G'$. 因此 $H \trianglelefteq G$. 故 $S(G) \leqslant M$. □

11.10　循环子群或正规或正规化所有子群的 p 群

郭秀云等[73] 研究了每个循环子群或正规或正规化所有子群的有限群 (称之为 N 群). 注意到, 群 G 中正规化 G 的所有子群的元素构成 G 的特征子群. 记为 $N(G)$. 显然 $Z(G) \leqslant N(G)$. N 群的子群和商群还是 N 群. G 是 Dedekind 群当且仅当 $G = N(G)$. 因此, N 群可看作为 Dedekind 群的一种推广. 近年来, 郭秀云和他的学生在有限 p 群领域获得了丰富的成果, 见 [44], [74], [75], [156], [206], [221]—[225], [255], [281]—[285]. 本节介绍他们在文献 [73] 的结果.

定理 11.10.1　*设 G 是有限群. 则 G 是 N 群当且仅当 G 是幂零群, 它的所有 Sylow 子群是 N 群且至多一个 Sylow 子群不是 Dedekind 群.*

证明　设 G 是 N 群. 令 $P \in \mathrm{Syl}_p(G)$ 且 x 是 G 的 p 元素. 因为 $\langle x\rangle \trianglelefteq G$ 或 $x \in N(G)$, 故 $P\langle x\rangle$ 是 G 的 p 子群. 于是 $x \in P$ 且 $P \trianglelefteq G$. 由此可得 G 幂零. 设 P 和 Q 是 G 的两个不同的 Sylow 子群且 P 和 Q 都不是 Dedekind 群. 于是存在 $x \in P$, $y \in Q$ 使得 $\langle x\rangle \ntrianglelefteq P$ 和 $y \notin N(Q)$. 令 $g = xy$. 则 $\langle g\rangle = \langle x\rangle \times \langle y\rangle$. 若 $\langle g\rangle \trianglelefteq G$, 则 $\langle x\rangle \trianglelefteq G$, 矛盾. 若 $g \in N(G)$, 则 $y \in N(G)$, 从而 $y \in N(Q)$, 也是矛盾. 于是 G 不是 N 群, 矛盾.

反之, 若 G 的所有 Sylow 子群是 Dedekind 群, 则 G 也是 Dedekind 群. 设 G 恰有一个 Sylow 子群 P 不是 Dedekind 群. 则 $G = P \times H$, 其中 $(|P|, |H|) = 1$ 且 H 是 Dedekind 群. 由 [223] 中的引理 2.1 可得 $N(G) = N(P) \times H$. 设 $g \in G$. 则存在 $x \in P$, $y \in H$ 使得 $g = xy$ 且 $\langle g\rangle = \langle x\rangle \times \langle y\rangle$. 若 $\langle x\rangle \trianglelefteq P$, 则 $\langle g\rangle \trianglelefteq G$. 若 $\langle x\rangle \ntrianglelefteq P$, 则 $x \in N(P)$, 从而 $g \in N(G)$. □

引理 11.10.2　*设 P 是有限 p 群.*

(1) 若 $N(P) < P$, 则 $N(P)$ 交换;

(2) 若 P 是 N 群, 则 $c(P) \leqslant 2$.

证明　(1) 因为 $N(P)$ 是 Dedekind 群, 由 [193] 中的定理 5.3.7 和 [53] 中的定理 6.5.1 可得 $N(P)$ 交换.

(2) 若否, 存在 $x, y \in P$ 使得 $[x, y] \notin Z(P)$. 由 [198] 中的定理可知 $x, y \notin N(P)$. 从而 $\langle x\rangle$ 和 $\langle y\rangle$ 均在 P 中正规. 故 $\langle x, y\rangle$ 是非交换的亚循环群. 若 $\langle x, y\rangle \not\simeq \mathrm{Q}_8$, 由 [113] 可知, $\langle x, y\rangle = \langle a, b\rangle$, 其中 $\langle b\rangle \ntrianglelefteq P$. 由此推出 $b \in N(P)$, $[a, b] \in Z(P)$. 从而 $[x, y] \in Z(P)$, 矛盾. 因而 $\langle x, y\rangle \simeq \mathrm{Q}_8$ 且 $\langle x, y\rangle'$ 是 P 的 2 阶正规子群, 这隐含着 $[x, y] \in Z(P)$, 矛盾. □

由定理 11.10.1 和引理 11.10.2(2), 即得如下定理.

定理 11.10.3　*设 G 是有限群. 若 G 是 N 群, 则 $c(G) \leqslant 2$.*

为了确定 N 群的结构, 由定理 11.10.1 可知, 我们只需确定素数幂阶的非 Dedekind 的 N 群. 简称为 N^* 群, $G \in N^*$ 表示 G 是一个 N^* 群. 注意到, 若 $G \in N^*$, 则 $N(G) < G$.

引理 11.10.4 *设 P 是有限 p 群且 $P \in N^*$. 则对于 P 的任意包含 $N(P)$ 的子群 K 以及对于 $x \in P\backslash N(P)$ 均有 $N(K) = N(P)$, $o(x) > \exp(N(P))$ 且 $x \notin C_P(N(P))$.*

证明 显然, $N(P) \leqslant N(K)$. 另一方面, 对于 $z \in K\backslash N(P)$, 存在 $y \in P$ 使得 $\langle y\rangle^z \neq \langle y\rangle$. 于是 $y \in N(P)$, 从而 $y \in K$. 由此推出 $z \notin N(K)$, 故 $N(K) = N(P)$.

令 $x \in P$ 使得 $x \notin N(P)$ 和 $H = \langle N(P), x\rangle$. 则 $N(H) = N(P)$. 由 [16] 中的陈述 1.1 可得 $\exp(N(P)) < o(x)$. 若 $x \in C_P(N(P))$, 则 $x \in Z(H) \leqslant N(H) = N(P)$, 矛盾. □

引理 11.10.5 *设 H 是有限交换 p 群 A 的齐次循环群使得 $\exp(H) = \exp(A)$. 则存在 A 的某个子群 B 使得 $A = H \times B$.*

证明 令 $H = \langle x_1\rangle \times \langle x_2\rangle \times \cdots \times \langle x_n\rangle$. 对 n 归纳. 若 $n = 1$, 由 [115] 中的定理 2.14 可知, H 是 A 的直因子. 设 $n > 1$. 令 $H_1 = \langle x_1\rangle \times \cdots \times \langle x_{n-1}\rangle$. 考虑商群 A/H_1. 再由 [115] 中的定理 2.14 可知, 对 A 的某个子群 B_1 有 $A/H_1 = H/H_1 \times B_1/H_1$. 由归纳假设, 对 B_1 的某个子群 B 有 $B_1 = H_1 \times B$. 因而 $A = HB_1 = H \times B$. □

引理 11.10.6 (Iwasawa[93]) *非 Hamilton p 群 P 是模群当且仅当 $P = A\langle g\rangle$, 其中 A 是交换正规子群, 对所有的 $a \in P$, $a^g = a^{1+p^s}$, $s \geqslant 1$; 若 $p = 2$, 则 $s \geqslant 2$.*

引理 11.10.7 *设 P 是有限 p 群且 $P \in N^*$. 则 $P/N(P)$ 循环.*

证明 由 N 群定义可知, P 的任意两个子群可置换. 故 P 是模群. 由引理 11.10.6 可知, $P = A\langle g\rangle$, 其中 A, g 如引理 11.10.6 所示. 断言 $\mho_s(A)$ 循环.

若否, 不妨设 $A = \langle x_1\rangle \times \langle x_2\rangle$ 且 $o(x_i) > p^s, i = 1, 2$. 这意味着 $[x_i, g] \neq 1$, $i = 1, 2$. 若 $\langle g\rangle \trianglelefteq P$, 则 $[x_i, g] \leqslant \langle x_i\rangle \bigcap \langle g\rangle$. 因为 $\langle x_1\rangle \bigcap \langle g\rangle \leqslant \langle x_2\rangle \bigcap \langle g\rangle$ 或 $\langle x_2\rangle \bigcap \langle g\rangle \leqslant \langle x_1\rangle \bigcap \langle g\rangle$, 由此可得 $\langle x_1\rangle \bigcap \langle g\rangle = 1$ 或 $\langle x_2\rangle \bigcap \langle g\rangle = 1$, 从而 $[x_1, g] = 1$ 或 $[x_2, g] = 1$, 矛盾. 因而 $\langle g\rangle \ntrianglelefteq P$ 且 $g \in N(P)$. 由引理 11.10.2(1) 可知, $x_1, x_2 \notin N(P)$ 且 $N(P) \bigcap A = C_A(g)$. 显然 $C_A(g) = \{a \mid a \in A, a^{p^s} = 1\}$. 从而 $N(P) \bigcap A$ 是齐次循环群. 令 r 是使得 $x_1^{p^r} \in N(P)$ 的最小正整数. 则 $x_1^{p^{r-1}} \notin N(P)$. 由引理 11.10.4 得, $\exp(N(P)) < o(x_1^{p^{r-1}})$, 从而 $\exp(N(P)) \leqslant o(x_1^{p^r}) \leqslant \exp(N(P) \bigcap A)$. 由引理 11.10.5 可知, 存在 $B \leqslant N(P)$ 使得 $N(P) = (N(P) \bigcap A) \times B$, 从而 $P = AN(P) = A \rtimes B$. 注意到 $x_1 \notin Z(P)$. 故存在 $b \in B$ 使得 $[b, x_1] \neq 1$. 然而, 由 $x_2 b \notin N(P)$ 可得 $\langle x_2 b\rangle \trianglelefteq P$ 且 $(x_2 b)^{x_1} = x_2 b[b, x_1] \in \langle x_2 b\rangle$. 于是 $[b, x_1] \in \langle x_1\rangle \bigcap \langle x_2 b\rangle = 1$, 矛盾. 故断言成立.

因为 $\mho_s(A)$ 循环, $A = A_1 \times \langle x\rangle$, 其中 $A \leqslant Z(P)$ 且 $[x, g] \neq 1$. 令 $P_1 = \langle x, g\rangle$. 由 [113] 可知, P_1 同构于 Q_8 或两个循环子群的直积, 其中一个非正规. 若 $P_1 \simeq Q_8$, 则 $x^g = x^{1+2}$. 这与 $s \geqslant 2$ 矛盾. 因而 $P_1 = \langle x_1\rangle\langle g_1\rangle$, 其中 $\langle g_1\rangle \ntrianglelefteq P_1$. 由此可得

$g_1 \in N(P)$. 从而 $P/N(P)$ 循环. $\square$

定理 11.10.8 设 P 是有限 p 群. 则 $P \in N^*$ 当且仅当 $P = \langle B, g\rangle \ltimes \langle x\rangle$, 其中 $\langle B, g\rangle$ 是由子群 B 和元 g 生成的交换群, $\langle x\rangle \trianglelefteq P$, 且 B, g 和 x 满足下列性质.

(i) $o(x) = p^{n+m}, o(g) = p^r, 1 \leqslant m \leqslant r \leqslant n+1-m, \exp(B) \leqslant p^{n+1-m}$, 若 $p = 2$, 则 $n + m \geqslant 3$;

(ii) $x^g = x^{1+p^n}$, $[B, x] = 1$.

证明　设 $P \in N^*$. 由引理 11.10.7 可知, 存在 $x \in P$ 使得 $x \notin N(P)$ 且 $P = N(P)\langle x\rangle$. 设 $N(P) \bigcap \langle x\rangle = \langle x^{p^m}\rangle$. 则 $m \geqslant 1$. 由引理 11.10.4 可知, x^{p^m} 是 $N(P)$ 的最大阶元, 故存在 $N(P)$ 的某个子群 T 使得 $N(P) = T \times (N(P) \bigcap \langle x\rangle)$. 因而 $P = T \ltimes \langle x\rangle$. 若 T 有元 b 使得 $x^b = x^{-1}$, 则 $(bx)^2 = b^2$. 然而, 因为 $bx \notin N(P)$, 由引理 11.10.4 可知 $o(b) < o(bx)$, 矛盾. 由 [115] 中的定理 2.19 推出 $T/C_T(x)$ 循环且当 $p = 2$ 时, $o(x) \geqslant 8$. 令 $B = C_T(x)$. 则存在 $g \in T$ 使得 $T = \langle B, g\rangle$, 其中 $[B, x] = 1$.

显然, $C_{\langle x\rangle}(g) = \langle x\rangle \bigcap Z(P) = \langle x\rangle \bigcap N(P) = \langle x^{p^m}\rangle$. 设 $o(x^{p^m}) = p^n$. 则 $n \geqslant 1$ 且 $o(x) = p^{n+m}$. 再设 $\langle [x, g]\rangle = \langle x^{p^i}\rangle, i \geqslant 0$. 则存在与 p 互素的整数 k 使得 $[x, g]^k = x^{p^i}$ 或 $[x, g^k] = x^{p^i}$. 用 g^k 替换 g, 不妨设 $[x, g] = x^{p^i}$. 从而 $x^g = x^{1+p^i}$. 因为 $C_{\langle x\rangle}(g) = \langle x^{p^m}\rangle$, 故 $i = n$. 因而 $x^g = x^{1+p^n}$. 由引理 11.10.2(2) 可得, $x^{p^n} \in \langle x\rangle \bigcap Z(P) = \langle x^{p^m}\rangle$. 从而 $n \geqslant m$.

令 $o(g) = p^r$. 易验证 g 在 $\langle x\rangle$ 上诱导一个 p^m 阶自同构. 故 $r \geqslant m$. 因为 $x^{p^{m-1}} \notin N(P)$, 故 $gx^{p^{m-1}} \notin N(P)$ 且 $\langle gx^{p^{m-1}}\rangle \trianglelefteq P$. 于是存在 $j \in Z$ 使得 $(gx^{p^{m-1}})^x = (gx^{p^{m-1}})^j$. 从而

$$gx^{-p^n}x^{p^{m-1}} = g^j x^{jp^{m-1}} x^{\frac{1}{2}j(j-1)p^{n+m-1}}.$$

等价地有

$$1 \equiv j \pmod{p^r}, \quad -p^n + p^{m-1} \equiv jp^{m-1} + \frac{1}{2}j(j-1)p^{n+m-1} \pmod{p^{n+m}}.$$

若 $r > n + 1 - m$, 则 $1 \equiv j \pmod{p^{n+2-m}}$. 由上述第二个同余式推出 $-p^n \equiv 0 \pmod{p^{n+1}}$, 矛盾. 因而 $r \leqslant n + 1 - m$. 令 $b \in B$ 和 $g_1 = bg$. 则 $x^{g_1} = x^{1+p^n}$. 类似地有 $o(g_1) \leqslant p^{n+1-m}$. 于是 $o(b) \leqslant p^{n+1-m}$. 由此推出 $\exp(B) \leqslant p^{n+1-m}$.

反之, 令 $P = \langle B, g\rangle \ltimes \langle x\rangle$ 是具有定理中所述性质的群. 显然地, $n \geqslant m$ 或当 $p = 2$ 时有 $n > m$. 易验证 $\langle x\rangle \bigcap Z(P) = \langle x^{p^m}\rangle$ 且 $P' = \langle [x, g]\rangle = \langle x^{p^n}\rangle \leqslant Z(P)$. 令 $y \in P$. 则 y 可表为 bg^kx^i 的形式, 其中 $b \in B$, $k, i \in Z$. 一方面, $y^g = bg^kx^{i(1+p^n)}$.

另一方面,

$$\begin{aligned} y^{1+p^n} = y(bg^k x^i)^{p^n} &= yg^{kp^n} x^{ip^n} [x^i, g^k]^{p^n(p^n-1)/2} \\ &= yx^{ip^n} (x^{ik})^{p^{2n}(p^n-1)/2} \\ &= bg^k x^{i(1+p^n)}. \end{aligned}$$

因而对任意的 $y \in P$ 有 $y^g = y^{1+p^n}$. 故 $g \in N(P)$. 进一步地, 因为 $[g, x^{p^{m-1}}] \neq 1$, 故 $x^{p^{m-1}} \notin N(P)$. 从而 $N(P) \bigcap \langle x \rangle = \langle x^{p^m} \rangle$ 且 $N(P) = \langle B, g \rangle \times \langle x^{p^m} \rangle$. 令 h 是 P 的使得 $h \notin N(P)$ 的一个元. 则 h 可表为 $bg^k x^{tp^l}$ 的形式, 其中 $b \in B$, $k, t, l \in Z$, $(t, p) = 1$, $0 \leqslant l < m$. 故

$$h^x = b(g[g, x])^k x^{tp^l} = bg^k x^{tp^l} x^{-kp^n} = hx^{-kp^n}.$$

令 $i = 1 - \delta p^{n-l}$, 其中 δ 是使得 $t\delta \equiv k \pmod{p^m}$ 的整数. 注意到 $n - l \geqslant n + 1 - m$. 我们有

$$\begin{aligned} h^i = h(bg^k x^{tp^l})^{-\delta p^{n-l}} &= hx^{-t\delta p^n} [g^{-k}, x^{-tp^l}]^{\delta p^{n-l}(\delta p^{n-l}-1)/2} \\ &= hx^{-t\delta p^n} x^{-kt\delta p^{2n}(\delta p^{n-l}-1)/2} \\ &= hx^{-kp^n} \\ &= h^x. \end{aligned}$$

因而 $\langle h \rangle \trianglelefteq P$ 且 $P \in N^*$. □

推论 11.10.9 设 P 是有限 p 群且 $P \in N^*$. 则 $|P : N(P)| = |N(P) : Z(P)| = \exp(P')$.

推论 11.10.10 对于任意一个素数 p 和任意一个非负整数 m, 存在一个有限 p 群 P 是 N 群且满足 $|P : N(P)| = p^m$.

推论 11.10.11 设 P 是有限 p 群满足 $|P : N(P)| = p$. 则 $P = R \times A$, 其中 $R = \langle x, u \mid x^{p^{n+1}} = u^{p^k} = 1,\ x^u = x^{1+p^n} \rangle$, $1 \leqslant k \leqslant n$, 若 $p = 2$, 则 $n \geqslant 2$, A 是交换群且 $\exp(A) \leqslant p^n$.

证明 显然, $P \in N^*$. 于是存在 $B \leqslant P$ 且 $g, x \in P$ 使得 $P = \langle B, g \rangle \ltimes \langle x \rangle$, 其中 $\langle B, g \rangle$ 交换, 且 B 和 g, x 具有定理 11.10.8 所述的性质. 因为 $|P : N(P)| = p^m$, 故 $m = 1$. 由此可得, $o(x) = p^{n+1}, o(g) = p^r, x^g = x^{1+p^n}, 1 \leqslant r \leqslant n$, $\exp(B) \leqslant p^n$, 且当 $p = 2$ 时有 $n \geqslant 2$. 注意到 $g^p \in Z(P)$. 不妨设 $g^p \in B$. 断言: 存在 $A \leqslant B$ 和 $u \in \langle B, g \rangle$ 使得 $\langle B, g \rangle = A \times \langle u \rangle$ 且 $x^u = x^{1+p^n}$. 事实上, 若 g^p 是 B 的极大阶元, 则对某个 $A \leqslant B$ 有 $B = A \times \langle g^p \rangle$. 从而 $\langle B, g \rangle = A \times \langle g \rangle$. 在这种情形下, 令 $u = g$. 则断言得证. 若 g^p 不是 B 的极大阶元, 取 $b \in B$ 使得 b 是 B 的极大阶元.

对某个 $B_1 \leqslant B$, 令 $B = \langle b \rangle \times B_1$. 则 g^p 可表为 $b^{tp}b_1$ 的形式, 其中 $t \in Z$, $b_1 \in B_1$. 令 $g_1 = b^{-t}g$. 显然, $g_1 \notin B, g_1^p \in B_1$, $\langle B, g \rangle = (\langle b \rangle \times B_1)\langle g_1 \rangle = \langle b \rangle \times \langle B_1, g_1 \rangle$, 且 $x^{g_1} = x^{1+p^n}$. 归纳可知, $\langle B_1, g_1 \rangle$ 有子群 $A_1 \leqslant B_1$ 和元 u 使得 $\langle B_1, g_1 \rangle = A_1 \times \langle u \rangle$ 且 $x^u = x^{1+p^n}$. 令 $A = \langle b \rangle \times A_1$. 则 $\langle B, g \rangle = A \times \langle u \rangle$, 判断得证. 再令 $R = \langle x, u \rangle$. 则 $P = \langle B, g \rangle \ltimes \langle x \rangle = A \times R$ 如所求. □

11.11 交换子群均为TI子群的 p 群

群 G 的子群 H 称为TI **子群**, 若对于任意的 $x \in G$ 均有 $H \bigcap H^x = 1$ 或 H. 显然, 正规子群是 TI 子群. 众所周知, 每个子群均正规的有限群被 Dedekind 研究并确定. Walls[220] 确定了每个子群是 TI 子群的群. 注意到, 每个交换子群是正规的群是 Dedekind 群. 李世荣等在文献 [131] 中分类了每个交换子群是 TI 子群的有限 p 群. 为方便, 以 $\mathcal{F}_p$ 表示每个交换子群是 TI 子群的有限 p 群类. $G \in \mathcal{F}_p$ 表示 G 是 $\mathcal{F}_p$ 群. 本节介绍他们的工作.

下面的两个引理结论显然的, 证明略去.

引理 11.11.1 设 G 是有限 p 群. 若 G 的所有交换子群是正规的, 则

(1) 若 p 是奇素数, 则 G 交换;

(2) 若 $p = 2$ 且 G 非交换, 则 $G \cong \mathrm{Q}_8 \times A$, 其中 A 初等交换.

引理 11.11.2 (1) $\mathcal{F}_p$ 是子群闭的, 即若 $G \in \mathcal{F}_p$ 且 $H \leqslant G$, 则 $H \in \mathcal{F}_p$;

(2) 若 H 是 G 的 TI 子群且 $H_G \neq 1$, 则 $H \lhd G$.

引理 11.11.3 $\mathrm{M}_p(n,1)$ 与 $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n}$ 均属于 $\mathcal{F}_p$.

证明 不妨设 $G = \mathrm{M}_p(n,1) = \langle a, b \mid a^{p^n} = b^p = 1, b^{-1}ab = a^{1+p^{n-1}} \rangle$, $n \geqslant 2$. 因为 $b^{-1}a^pb = a^{(1+p^{n-1})p} = a^p$, 故 $Z(G) = \langle a^p \rangle$ 在 G 中的指数为 p^2. 由此可得 $G' \subseteq Z(G)$. 因为 $c(G) = 2$, 故 $[a,b]^p = [a^p, b] = 1$. 从而 $G' = \langle [a,b] \rangle$ 且 $|G'| = p$. 令 S 是 G 的阶大于 p 的交换子群. 则 $S \bigcap Z(G) \neq 1$. 因而 $G' \leqslant S$ 且 $S \unlhd G$. 由此得 $G \in \mathcal{F}_p$. 类似论证可得, $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n} \in \mathcal{F}_p$. □

注意: $\mathrm{M}_p(n,1)$ 与 $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n}$ 在文献 [131] 中分别被表示为 $G(p^n, p)$ 与 $G(p, p, p^n)$.

下面我们分类 $\mathcal{F}_p$ 群.

定理 11.11.4 $G \in \mathcal{F}_p$ (p 是奇素数) 当且仅当 G 是下列互不同构的群之一.

(1) G 交换;

(2) $G = \mathrm{M}_p(n,1)$, $m \geqslant 2$;

(3) $G = \mathrm{M}_p(1,1,1) * \mathrm{C}_{p^n}$, $n \geqslant 1$.

证明 $\Longleftarrow$: 若 G 交换, 显然 $G \in\in \mathcal{F}_p(p)$. 引理 11.11.3 保证了群 (2) 和 (3) 属于 $\mathcal{F}_p$. 定理中的群互不同构是显然的.

$\Longrightarrow$: 设 G 是非交换的 $\mathcal{F}_p$ 群. 令 Z 是 $Z(G)$ 的 p 阶子群. 由引理 11.11.2(2) 可知, G/Z 的每个循环子群皆正规. 由于 $p>2$, 故 G/Z 交换. 于是 $Z(G)$ 循环且 $|G'|=p$. 又 G 非交换, 由定理 1.10.1 知, 存在 G 的 p 阶子群 U 使得 U 不在 $Z(G)$ 中. 令 $S=ZU=Z\times U$. 由 $G'=Z$ 得, $S\trianglelefteq G$. 于是 $G/C_G(U)=G/C_G(S)$ 同构于 $\mathrm{Aut}(S)$ 的某个子群. 众所周知, $\mathrm{Aut}(S)\cong \mathrm{GL}(2,p)$ 且 $|\mathrm{GL}(2,p)|=p(p-1)(p^2-1)$. 由此推出 $|G/C_G(U)|=p$. 故 $C_G(U)$ 是 G 的极大子群. 由引理 11.11.2 得 $C_G(U)\in\mathcal{F}_p$. 因为 $Z(C_G(U))$ 非循环, 故 $A:=C_G(U)$ 交换. 从而对 G 的某个循环子群 $\langle b\rangle$ 有 $G=\langle b\rangle A$.

断言 $G=\langle a,b,Z(G)\rangle$: 事实上, 由定理 1.7.5 得, 映射 $\phi: a\mapsto [a,b]$ 是 A 到 G' 的满同态. 因为 $|G'|=p$, 故对某个固定的 $a\in A$ 有 $G'=\langle [a,b]\rangle$. 注意到 $Z(G)$ 循环且 A 交换. 故 $Z(G)\subseteq A$. 显然 $\ker\phi=Z(G)$. 因而 $A/Z(G)\cong G'$, 且 $|A/Z(G)|=p$. 令 $A=\langle a\rangle Z(G)$. 则 $G=\langle a,b,Z(G)\rangle$, 且 $|G:Z(G)|=p^2$. 于是断言被证明.

若 $\langle a,Z(G)\rangle$ 或 $\langle b,Z(G)\rangle$ 循环, 则 G 有循环极大子群. 由定理 1.9.1 即得 $G\cong \mathrm{M}_p(n,1)$.

设 $\langle a,Z(G)\rangle$ 和 $\langle b,Z(G)\rangle$ 均不循环. 于是 $\langle a,Z(G)\rangle$ 至少有两个不同的 p 阶子群. 不妨设 $a^p=1$. 同理 $b^p=1$. 故 $G=\langle a,b,Z(G)\rangle=Z(G)\langle a,b\rangle$. 现在容易看到 $\langle a,b\rangle$ 是 p^3 阶非交换群且 $|[a,b]|=p$. 令 $Z(G)=\langle z\rangle$. 明显地, $\langle z^{p^{n-1}}\rangle$ 是 G 的唯一的 p 阶正规子群. 故对某个满足 $(k,p)=1$ 的 k 有 $[a,b]=z^{kp^{n-1}}$. 用 z^k 替换 z 得, $[a,b]=z^{p^{n-1}}$. 现在得到 G 是群 (3). □

引理 11.11.5 *设 $G\in\mathcal{F}_2$, Z 是 $Z(G)$ 的 2 阶子群. 若 G/Z 是 Hamilton 群, 则 G 也是 Hamilton 群.*

证明 由引理 11.11.1, 不妨设 $G/Z=H/Z\times A/Z$, 其中 $H/Z\cong \mathrm{Q}_8$, A/Z 初等交换.

首先断言 $H=\mathrm{Q}_8\times Z$: 事实上, 由引理 11.11.2 得 $H\in\mathcal{F}_2$. 令 V 是 H 的交换子群. 我们将证明 $V\trianglelefteq H$. 首先观察到, 由 Q_8 的每个极大子群循环可得, H 的包含 Z 的极大子群交换. 于是 $|H:Z(H)|=4$. 若 $|V|\geqslant 4$, 则 $V\bigcap Z(H)\neq 1$. 特别地, $V_H\neq 1$. 由此可得 $V\trianglelefteq H$. 若 $|V|=2$ 且 $V\neq Z$, 则 VZ/Z 是 H/Z 的唯一的 2 阶子群. 故 $VZ/Z\leqslant \Phi(H/Z)$. 于是 $V\subseteq Z(H)$, 从而也有 $V\trianglelefteq H$. 由引理 11.11.1 即得 $H=\mathrm{Q}_8\times Z$.

其次证明 $\mathrm{Q}_8\trianglelefteq G$: 若 $A=Z$, 结论成立. 设 $A>Z$. 因为 A/Z 初等交换, 只需证 A 的所有包含 Z 的 4 阶子群正规化 Q_8 即可. 记 $K=\mathrm{Q}_8U$. 则 $U\lhd K$ 且 $K/C_K(U)$ 同构于 $\mathrm{Aut}(U)$ 的一个子群. 因为 $|U|=4$, 故 $|\mathrm{Aut}(U)|_2=2$. 从而 $|K/C_K(U)|=2$. 于是 $C_K(U)$ 包含 Q_8 的一个 4 阶循环子群. 特别地, $Z(\mathrm{Q}_8)\leqslant Z(K)$. 从而对于 Q_8 的每个 4 阶循环子群均有 $V_K\neq 1$. 另一方面, 由引理 11.11.2 得 $K\in\mathcal{F}_2$. 由 $\mathcal{F}_2$ 群的定义可知, 对于 Q_8 的每个 4 阶循环子群均有 $V\trianglelefteq K$. 故 $\mathrm{Q}_8\trianglelefteq K$.

最后断言 A 初等交换: 若否, 则存在 4 阶元 $u \in A$ 使得 $Z = \langle u^2 \rangle$. 记 $U = \langle u \rangle$. 由上述断言知 $G = \mathrm{Q}_8 \times A$. 设

$$\mathrm{Q}_8 = \langle a, b \mid a^4 = b^4 = 1, a^2 = b^2, a^b = a^{-1} \rangle.$$

令 $x = au$ 且 $X = \langle x \rangle$. 则 $x^2 = (au)^2 = a^2u^2 \neq 1$. 显而易见, a^2 和 u^2 在 $Z(G)$ 中. 于是 $X_G \neq 1$. 由假设得 $X \trianglelefteq G$. 于是对某个整数 r,

$$a^{-1}u = a^b u^b = (au)^b = (au)^r = a^r u^r,$$

这意味着 $a^{r+1} = u^{1-r}$. 从而推出 $4 \mid (r+1)$ 且 $4 \mid (1-r)$, 矛盾. 因而 A 初等交换.

综上所述, $G = \mathrm{Q}_8 \times A$. 故 G 是 Hamilton 群. □

引理 11.11.6　*设 $G \in \mathcal{F}_2$. 若 G 有一个不在 $Z(G)$ 中的 2 阶元 u 使得 $C_G(u)$ 非交换, 则 $G = \mathrm{Q}_8 * \mathrm{D}_8$.*

证明　显而易见, 对于 $Z(G)$ 的任何一个 2 阶子群 Z, G/Z 的每个循环子群正规. 由引理 11.11.5 可知, G/Z 交换. 故 $Z(G)$ 循环. 记 $M = C_G(u)$, 其中 u 是不在 $Z(G)$ 中的 2 阶元. 与定理 11.11.4 的论证类似可证, $|G : M| = 2$. 又由引理 11.11.2 得 $M \in \mathcal{F}_2$. 若 $M/\langle u \rangle$ 交换, 则由 M/Z 交换及 $\langle u \rangle \bigcap Z = 1$ 可得 M 交换. 与假设矛盾. 故 $M/\langle u \rangle$ 非交换, 从而 $M/\langle u \rangle$ 是 Hamilton 群. 由引理 11.11.5 可得 $M = \mathrm{Q}_8 \times A$, 其中 A 初等交换且 $Z \leqslant \mathrm{Q}_8$.

断言 $|A| = 2$: 事实上, 因为 $|G : M| = 2$, 故对 $x \in G \backslash M$ 有

$$(A \bigcap A^x)^x = A^x \bigcap A^{x^2} = A^x \bigcap A.$$

故 $A \bigcap A^x \trianglelefteq G$. 若 $A \bigcap A^x \neq 1$, 则 $A \bigcap A^x$ 包含 $Z(G)$ 的一个 2 阶子群. 于是由 Z 是 $Z(G)$ 的唯一 2 阶子群推出 $Z \leqslant A$, 矛盾. 故 $A \bigcap A^x = 1$. 从而 $AA^x = A \times A^x \leqslant \Omega_1(M)$. 另一方面, $\Omega_1(M) = Z \times A$. 比较阶可得 $|A| = 2$.

设 $u \in A$. 则 $\Omega_1(M) = Z \times \langle u \rangle \subseteq Z(M)$ 且 $|G| = 2^5$. 若 $\Omega_1(M) = \Omega_1(G)$, 则对于 $x \in G \backslash M$ 有 $|x| > 2$. 因为 $\exp(M) = 4$, 故 $4 \leqslant \exp(G) \leqslant 8$. 记 $X = \langle x \rangle$. 若 $|X| = 4$, 则 $x^2 \in \Omega_1(M) \leqslant Z(M)$. 于是 $x^2 \in Z(G)$, 从而 $X \lhd G$. 显然, $\langle u \rangle X = \mathrm{D}_8$. 这意味着 M 外有一个对合, 矛盾. 于是 $|X| = 8$. 注意到 Q_{2^4} 的导群是 4 阶的, 而 $|G'| = 2$. 由此可知 G 没有子群同构于 Q_{2^4}. 其次, 考虑子群 $G_1 = \langle a, x \rangle$ 和 $G_2 = \langle b, x \rangle$, 其中 a 和 b 是 Q_8 的生成元. 易证 G_1 和 G_2 均非循环. 故 $\Omega_1(M) \leqslant G_i$, 从而 $\langle u, x \rangle \leqslant G_i, i = 1, 2$. 比较阶可得, $\langle a, x \rangle = \langle u, x \rangle = \langle b, x \rangle$. 这意味着 $G = \langle u, x \rangle$ 且 $|G| = 2^4$. 这与 $|G| = 2^5$ 矛盾. 因而 $\Omega_1(M) < \Omega_1(G)$.

在此情形下, G 由一个 2 阶元 $v \in G \backslash M$. 则 $G = (\mathrm{Q}_8 \times \langle u \rangle) \rtimes \langle v \rangle$. 因为 G/Z 交换, 故 $\langle u \rangle Z \trianglelefteq G$, $\langle v \rangle Z \trianglelefteq G$. 于是 $\langle u, v \rangle = \mathrm{D}_8$. 因而 $G = \mathrm{Q}_8 * \mathrm{D}_8$. 易验证 $\mathrm{Q}_8 * \mathrm{D}_8$ 的交换子群是 TI 子群. □

定理 11.11.7 设 G 是有限 2 群. 则 $G\in\mathcal{F}_2$ 当且仅当 G 是下列互不同构的群之一.

(1) 交换 2 群;

(2) Hamilton 2 群;

(3) $\mathrm{Q}_8*\mathrm{D}_8$;

(4) $\mathrm{M}_2(n,2)$;

(5) $\mathrm{M}_2(1,1,1)*\mathrm{C}_{2^n}$.

证明 $\Longleftarrow$: 容易验证定理中的群属于 $\mathcal{F}_2$.

$\Longrightarrow$: 设 G 是非交换的 $\mathcal{F}_2$ 群使得 G 既不是群 (2) 也不是群 (3). 由引理 11.11.5 和 11.11.6 可知,

(C_1): 对于 G 的任意一个 2 阶子群 Z 均有 G/Z 交换;

(C_2): 对于 G 的任意一个不在 $Z(G)$ 的 2 阶元 u 均有 $M=C_G(u)$ 交换.

进一步地, G 有一个子群 M 满足 (C_2). 由 (C_1) 可知, $Z(G)$ 循环. 又由 (C_2) 得, M 交换且 $|G:M|=2$.

与定理 11.11.4 的论证类似可证, $G=\langle a,b,Z(G)\rangle$ 且 $|G:Z(G)|=2^2$.

若 $\langle a,Z(G)\rangle$ 或 $\langle b,Z(G)\rangle$ 循环, 则 G 有循环极大子群. 由定理 1.9.1 及 $|G'|=2$ 即得 $G\cong\mathrm{M}_2(n,1)$.

若 $\langle a,Z(G)\rangle$ 和 $\langle b,Z(G)\rangle$ 均不循环, 与定理 11.11.4 的论证类似可证, $G\cong\mathrm{M}_2(1,1,1)*\mathrm{C}_{2^n}$, $n\geqslant 2$. □

11.12 子群均共轭置换的 p 群

我们知道, 正规子群是有限群的一个核心概念. Ore 于 1937 年在文献 [172] 引进了一个比正规子群更弱的概念, 即**拟正规子群**. 称群 G 的子群 H 为 G 的拟正规子群 (quasinormal subgroup) 或**置换子群**(permutable subgroup), 如果对 G 的任意一个子群 K 均有 $HK=KH$. Ore 证明了拟正规子群必次正规. 之后, 对置换子群的研究颇为活跃, 可见文献 [39], [54], [55], [58], [70], [71], [92], [168]—[171], [211]—[215], [217], [268] 等.

Foguel 观察到, 在证明拟正规子群 H 是次正规子群的过程中, 只需证明 H 与它的所有共轭子群可交换. 于是他在文献 [65] 中引进了一个新的子群概念, 即**共轭置换子群**. 称群 G 的子群 H 为 G 的共轭置换子群 (conjugate permutable subgroup), 如果对 G 的任意一个元 g, 均有 $HH^g=H^gH$. 记为 $H<_{C-P}G$. 显然, 拟正规子群必共轭置换. Foguel 在文献 [65] 证明了共轭置换子群必次正规. 他也给出例子表明次正规未必共轭置换, 共轭置换未必拟正规. 文献 [66] 对共轭子群开展了进一步的研究. 徐明曜等在文献 [245] 利用某些子群的共轭置换性给出了有限群为幂零、

超可解等结果. 研究了每个子群为共轭置换的有限群, 他们称这样的群为 ECP 群. 文献 [245] 给出了几类 ECP p 群. 之后, 李世荣等在文献 [130] 引进了自共轭置换子群的概念. 称群 G 的子群 H 为 G 的自共轭置换子群 (self-conjugate permutable subgroup), 如果 $HH^g = H^gH$, 则 $H^g = H$. 文献 [130] 研究了共轭置换子群和自共轭置换子群的某些性质, 描述了所有循环子群是自共轭置换的有限群以及所有循环子群是共轭置换或自共轭置换的有限群. 本节主要介绍 ECP p 群的某些结果.

定理 11.12.1 *有限群 G 是 ECP 群当且仅当 G 是幂零群且 G 的每个 Sylow p子群是 ECP 群.*

证明 $\Longrightarrow$: 注意到每个子群必次正规, 结论是显然的.

$\Longleftarrow$: 设 $H \leqslant G$, $G = P_1 \times P_2 \times \cdots \times P_s$, 其中 $\{P_i\}$ 是 G 的 Sylow p 子群. 对每个 i, 令 $H_i = H \bigcap P_i$. 则 $H = H_1 \times H_2 \times \cdots \times H_s$. 使用归纳易得 $H <_{C-P} G$. □

定理 11.12.2 *幂零类为 2 的有限 p 群 G 是 ECP 群.*

证明 设 $H \leqslant G$, $g \in G$, $h, h' \in H$. 因为 $c(G) = 2$, 故 $[h, g] \in Z(G)$. 对任意的 $h^gh' \in H^gH$, 有

$$h^gh' = h[h,g]h' = hh'h^{-1}h[h,g] = {h'}^{h^{-1}}h^g \in HH^g.$$

于是 $H^gH \subseteq HH^g$. 因为 $|H^gH| = |HH^g|$, 故 $H^gH = HH^g$, 即 H 是共轭置换的. □

Mann 在文献 [153] 中的问题 3 猜想: 大多数 p 群是类 2 的. 如果这个猜想是正确的, 那么大多数 p 群是 ECP 群.

定理 11.12.3 *设 p 为奇素数. 则导群循环的有限 p 群是 ECP 群. 特别地, 奇数阶亚循环 p 群是 ECP 群.*

证明 对 $|G|$ 作归纳. 若 $|G| \leqslant p^2$, 则 G 交换, 结论明显成立. 假设 $|G| \geqslant p^3$ 且 $H \leqslant G$. 要证 $H <_{C-P} G$. 若 $K := \mathrm{Core}(H) \neq 1$, 由归纳假设可得, $H/K <_{C-P} G/K$. 从而 $H <_{C-P} G$. 不妨设 $K = 1$. 若 H 不是共轭置换的, 则存在 $g \in G$ 使得 $HH^g \neq H^gH$. 于是存在 $h \in H$ 使得 $[h, g] \neq 1$. 由 [89] 中的 III, 定理 10.13 可知, G 正则. 设 $[h, g]^{p^s} = 1$, 其中 s 为正整数. 由 [89] 中的 III, 定理 10.6(b) 可知, $[h^{p^{s-1}}, g]^p = 1$. 令 $x = [h^{p^{s-1}}, g]$. 则 $\Omega_1(G') = \langle x \rangle$ 且 $x \in HH^g$. 因为 $|\Omega_1(G')| = p$, 故 $x \in Z(G)$. 于是对满足 $1 \leqslant i \leqslant p-1$ 的每个 i, 都有 $x^i = [h^{ip^{s-1}}, g] \in HH^g$. 因而 $HH^g \geqslant \Omega_1(G')$. 类似地有 $H^gH \geqslant \Omega_1(G')$. 令

$$\overline{G} = G/\Omega_1(G'), \quad \overline{H} = H\Omega_1(G')/\Omega_1(G').$$

由归纳假设可得

$$H\Omega_1(G')/\Omega_1(G') \cdot H^g\Omega_1(G')/\Omega_1(G') = H^g\Omega_1(G')/\Omega_1(G') \cdot H\Omega_1(G')/\Omega_1(G').$$

于是 $HH^g\Omega_1(G')=H^gH\Omega_1(G')$. 因为 $HH^g \geqslant \Omega_1(G')$ 且 $H^gH \geqslant \Omega_1(G')$, 故 $HH^g = H^gH$, 矛盾. □

每个循环子群为共轭置换的有限群称为 CCP 群. Foguel 在 [66] 证明了: 方次数 p 的有限群是 CCP 群当且仅当 G 满足 2-Engel 条件. 对于 ECP 群, 则有下列结论.

定理 11.12.4 设 G 是方次数 p 的有限群且 $p \neq 3$. 则 G 是 ECP 群当且仅当 $c(G) \leqslant 2$.

证明 若 $p = 2$, 则 G 交换. 故 G 是 ECP 群. 不妨设 $p > 3$. 若 G 是 ECP 群, 则 G 是 CCP 群. 于是 G 满足 2-Engel 条件. 由 [89] 中的 III, 定理 6.5 可知, $c(G) \leqslant 2$. 反之, 由定理 11.12.2 可得结论. □

若 $p = 3$, 则方次数 p 的有限群 G 满足 2-Engel 条件, 但它的幂零类可以是 3. 然而, G 是 CCP 群. 一个自然的问题是: 方次数 3 的有限群是 ECP 群吗? 这是一个未解决的问题.

定理 11.12.5 设 $p \geqslant 5$. 则 ECP p 群是正则的.

证明 若否, 设 G 是极小阶反例. 则 G 是极小非正则的. 由 [247] 中的定理 5.2.15 可知, $\mho_1(G) \leqslant Z(G)$. 因为 $\exp(G/\mho_1(G)) = p$, 由定理 11.12.4 可知, $c(G/\mho_1(G)) \leqslant 2$, 因而 $c(G) \leqslant 3$. 由此可得 G 正则, 矛盾. □

一个自然的问题是: 对于 $p = 3$, 每个 ECP p 群是正则的吗? 这也是一个未解决的问题.

对于有限群, Foguel 在文献 [65] 证明了共轭置换子群必次正规. 对于无限群, 李世荣等在文献 [130] 证明了下列定理.

定理 11.12.6 设 G 的子群满足极大条件和极小条件. 则 G 的共轭置换子群必次正规.

证明 设 $H <_{C-P} G$ 且 $H \ntrianglelefteq G$. 则存在 $x_1 \in G$ 使得 $H^{x_1} \neq H$. 令 $K_1 = HH^{x_1}$. 由 [65] 中的引理 1.1 可知, $K_1 <_{C-P} G$ 且 $H < K_1$. 若 $H \ntriangleleft K_1$, 则存在 $x_2 \in K_1$ 使得 $H^{x_2} \neq H$. 令 $K_2 = HH^{x_2}$. 则 $K_2 <_{C-P} G$ 且 $K_2 < K_1$. 于是我们有 $K_1 > K_2 > H$. 若 $H < HH^y$ 总有 $H \ntriangleleft HH^y$, 则重复上述过程, 我们得到一个无限长的子群列

$$G > K_1 > K_2 > \cdots > K_r > \cdots > H.$$

这与 G 的子群满足极小条件的假设矛盾. 因而不妨设 $H \lhd K_1$. 因为 $K_1 <_{C-P} G$, 对 K_1 应用上述做法, 若 $K_1 \ntriangleleft G$, 则存在 $x_2 \in G$ 使得 $K_1 < K_1K^{x_2}$ 且 $K_1 \lhd K_1K^{x_2}$. 令 $K_2 = K_1K^{x_2}$. 因为 G 的子群满足极大条件, 得到一个子群列

$$H = K_0 \lhd K_1 \lhd K_2 \lhd \cdots \lhd K_s \lhd G,$$

其中

$$K_1 = HH^{x_1}, \quad \text{对每个 } i, \quad K_i = K_{i-1}K_{i-1}^{x_i}, \quad \text{或} \quad K_i < K_{i+1}.$$

这就证明了 H 在 G 中次正规. □

11.13 奇素数幂阶 J 群的分类

在 2000 年, Herzog, Longobardi, Maj 和 Mann 在文献 [82] 提出 J 群的概念并对其结构进行了研究. 回顾一下, 称群 G 为J 群($G \in J$), 若对任意的 $x \in G$, 或者 $\langle x\rangle \trianglelefteq G$, 或者对任意的 $g \in G \setminus N_G(\langle x\rangle)$ 有 $\langle x, x^g\rangle \trianglelefteq G$. 显然, Dedekind 群是 J 群. 正像文献 [82] 的作者所指出的, 有限 J 群的主要问题在于有限 p 群的结构问题. 他们证明了: 对于 $p > 2$, 若有限非交换 p 群是 J 群, 则 $c(G) \leqslant 3$, 而且若 $c(G) = 2$, 则 $|G'| \leqslant p^2$ 且 $\exp(G') = p$. 当 $c(G) = 3$ 时, 他们还证明了如下定理.

定理 11.13.1 [82]　*设 G 为有限 p 群, $p > 2$ 且 $c(G) = 3$. 则 G 是 J 群当且仅当 $p = 3$ 且 $G = AB$, 其中 A, B 满足下列条件:*

(a) $A = \langle a, b, c \mid a^9 = b^9 = c^3 = 1, a^3 = b^{-3}, [a, b] = c, [c, a] = a^{-3}, [c, b] = 1\rangle$;

(b) $c(B) \leqslant 2, \exp(B) = 3, B' \leqslant \langle a^3\rangle$ 且 $[B, a] = 1, [B, b] \leqslant \langle a^3\rangle$.

由此可见, 要确定奇素数幂阶的 J 群结构, 只需考虑类 2 的 J 群 G. 因为导群为素数阶的 p 群已被 Blackburn 在文献 [36] 分类, 故只需研究 $G' \cong \mathrm{C}_p \times \mathrm{C}_p$ 的情形. 在这种情形下, 显然 $d(G) \geqslant 3$. 依照 $d(G) = 3$ 和 $d(G) \geqslant 3$ 两种情形, 郭秀云等在文献 [74] 分类了这样的 J 群. 结果表明, 这类群与幂零类为 3 的 J 群有类似的结构. 本节介绍文献 [74] 的工作. 以下总假设 $p > 2$.

11.13.1　三元生成的素数幂阶 J 群

引理 11.13.2　*设 G 为有限 p 群. 若 $c(G) = 2$, 且 $G' \cong \mathrm{C}_p \times \mathrm{C}_p$, 则 G 必有三元生成的子群 K 满足 $K' = G'$.*

证明　因 G 非交换, 故存在元素 $a, b \in G$ 使得 $[a, b] \neq 1$. 若存在 $c \in G$ 使得 $[c, a] \notin \langle [a, b]\rangle$ 或 $[c, b] \notin \langle [a, b]\rangle$, 则 $K = \langle a, b, c\rangle \leqslant G$ 就满足 $K' = G'$. 不妨设对任意元素 $c \in G$ 都有 $[c, a] \in \langle [a, b]\rangle$ 且 $[c, b] \in \langle [a, b]\rangle$. 因 $G' \cong \mathrm{C}_p \times \mathrm{C}_p$, 故存在 $c, d \in G$ 使得 $[c, d] \notin \langle [a, b]\rangle$ 且 $G' = \langle [a, b], [c, d]\rangle$. 若 $[c, a] \notin \langle [c, d]\rangle$, 则取 $K = \langle a, d, c\rangle$ 即可. 进而可设 $[c, a] \in \langle [c, d]\rangle$. 注意到 $[c, a] \in \langle [a, b]\rangle$. 故 $[c, a] = 1$. 类似地, 可得 $[d, b] = 1$. 于是 $G' = \langle [a, b], [c, d]\rangle = \langle [bc, a], [bc, d]\rangle$. 因此 $K = \langle a, bc, d\rangle$ 即为所求. □

引理 11.13.3　*设 G 为有限 p 群, $c(G) = 2$ 且 $G' \cong \mathrm{C}_p \times \mathrm{C}_p$. 则 G 为 J 群当且仅当对 G 中满足 $\langle g\rangle \bigcap G' = 1$ 的所有元 g 都有 $|\langle [g, G]\rangle| \leqslant p$.*

证明　$\Longrightarrow$: 设 $g \in G$ 且 $\langle g\rangle \bigcap G' = 1$. 若 $\langle g\rangle \trianglelefteq G$, 则 $[g, G] \leqslant \langle g\rangle \bigcap G' = 1$. 现设 $\langle g\rangle \ntrianglelefteq G$. 由假设, 对任意 $a \in G - N_G(\langle g\rangle)$ 有 $\langle g, g^a\rangle \trianglelefteq G$. 于是对任意的 $b \in G$ 有

$[g,b]\in\langle g,g^a\rangle$. 这样就有 $[g,G]\leqslant\langle g,g^a\rangle\bigcap G'$. 又由 $c(G)=2$ 知, $\langle g,g^a\rangle=\langle g,[g,a]\rangle$ 为交换群, 故 $|[g,G]|\leqslant p$.

$\Longleftarrow$: 设 $g\in G$ 且 $\langle g\rangle\ntrianglelefteq G$. 又设 $a\in G\backslash N_G(\langle g\rangle)$. 若 $\langle g\rangle\bigcap G'=1$, 则 $[g,G]$=$\langle[g,a]\rangle$. 于是 $\langle g,g^a\rangle=\langle g,[g,a]\rangle\trianglelefteq G$. 若 $\langle g\rangle\bigcap G'\neq 1$, 则由 $G'\cong \mathrm{C}_p\times \mathrm{C}_p$ 知, 对任意元 $a\in G\backslash N_G(\langle g\rangle)$ 有 $G'=\langle\langle g\rangle\bigcap G',[g,a]\rangle\leqslant\langle g,g^a\rangle$. 从而 $\langle g,g^a\rangle\trianglelefteq G$. □

引理 11.13.4 下列群都是 J 群.

(Ⅰ) $\langle a,b,c\mid a^{p^n}=x,b^{p^m}=c^{p^s}=1,[a,b]=y,[a,c]=x,[b,c]=1,x^p=y^p=1,x,y\in Z(G)\rangle$, 其中 $n\geqslant s,n\geqslant m$;

(Ⅱ) $\langle a,b,c\mid a^{p^n}=x,b^{p^m}=y,c^{p^s}=1,[a,b]=x,[a,c]=1,[b,c]=y,x^p=y^p=1,x,y\in Z(G)\rangle$, 其中 $m\geqslant s$;

(Ⅲ) $\langle a,b,c\mid a^{p^n}=x,b^{p^m}=y,c^{p^s}=1,[a,b]=y,[a,c]=1,[b,c]=x,x^p=y^p=1,x,y\in Z(G)\rangle$, 其中 $m\geqslant s$.

不同类型的群或者相同类型不同参数的群互不同构.

证明 (1) 设 G 为 (Ⅰ) 型群. 若 $g\in G$ 且 $\langle g\rangle\bigcap G'=1$, 则 g 可写成 $a^{ip}b^jc^ky^l$ 的形式, 其中 i,j,k,l 为非负整数. 因为 $c(G)=2$ 且 $\exp(G')=p$, 故

$$[a^{ip}b^jc^ky^l,b]=[a^{ip}b^jc^ky^l,c]=1.$$

从而

$$|[a^{ip}b^jc^ky^l,G]|=|\langle[a^{ip}b^jc^ky^l,a]\rangle|\leqslant p.$$

由引理 11.13.3 知 G 为 J 群.

(2) 设 G 为 (Ⅱ) 型群. 若 $g\in G$ 且 $\langle g\rangle\bigcap G'=1$, 则 g 可写成 $a^ib^{jp}c^k$ 的形式, 其中 i,j,k 为非负整数. 由 $c(G)=2$ 和 $\exp(G')=p$ 知,

$$[a^ib^{jp}c^k,a]=[a^ib^{jp}c^k,c]=1.$$

从而

$$|[a^ib^{jp}c^k,G]|=|\langle[a^ib^{jp}c^k,b]\rangle|\leqslant p.$$

由引理 11.13.3 知 G 为 J 群.

类似可知 (III) 型群也是 J 群.

下面证明 (Ⅰ) 型群、(Ⅱ) 型群、(III) 型群是互不同构的.

设 G 为 (Ⅰ) 型群. 首先可证: 当参数取不同值时所对应的群是互不同构的. 事实上, (Ⅰ) 型群可以分为以下 A, B 两组

$\mathrm{A}(n,m,s;a,b,c)$=$\langle a,b,c\mid a^{p^n}=x,b^{p^m}=c^{p^s}=1,[a,b]=y,[a,c]=x,[b,c]=1,x^p=y^p=1,x,y\in Z(G)\rangle$, 其中 $n\geqslant m\geqslant s$.

$\mathrm{B}(n,s,m;a,b,c)=\langle a,b,c \mid a^{p^n}=x, b^{p^m}=c^{p^s}=1, [a,b]=y, [a,c]=x, [b,c]=1, x^p=y^p=1, x,y\in Z(G)\rangle$, 其中 $n\geqslant s>m$.

由 G/G' 的型不变量知, A, B 组内部是互不同构的. 故只需证 A, B 之间亦不同构. 若群 $\mathrm{A}(n,m,s;a,b,c)\cong \mathrm{B}(n_1,s_1,m_1;a_1,b_1,c_1)$, 由 G/G' 的型不变量知, $n_1=n, s_1=m, m_1=s$. 不妨设

$$a_1=a^{i_1}b^{j_1}c^{k_1},\quad c_1=a^{pi_2}b^{j_2}c^{k_2},\quad b_1=a^{pi_3}b^{pj_3}c^{k_3},$$

其中 $i_1,i_2,i_3,j_1,j_2,j_3,k_1,k_2,k_3$ 均为正整数. 计算 a_1,c_1 和 b_1 的阶可知, $p|i_2, p|i_3$, $p|j_3$ 且 $(i_1,p)=1$. 由 $b_1\notin\Phi(G)$ 知, $(k_3,p)=1$. 因为 $G/\Phi(G)$ 三元生成, 故 $(j_2,p)=1$. 因 $c(G)=2$, 故

$$y^{i_1j_2}x^{i_1k_2}=[a^{i_1},b^{j_2}c^{k_2}]=[a^{i_1}b^{j_1}c^{k_1},a^{i_2}b^{j_2}c^{k_2}]=[a_1,c_1]=a_1^{p^n}=x^{i_1}.$$

这就得到 $p|i_1j_2$. 与 $(i_1j_2,p)=1$ 矛盾.

用同样的方法可证, (Ⅱ) 型群、(Ⅲ) 型群内部也是互不同构的.

由 $|\mho_1(G)\bigcap G'|$ 知 (Ⅰ) 型群和 (Ⅱ), (Ⅲ) 型群不同构. 故只需证 (Ⅱ) 型群和 (Ⅲ) 型群之间是互不同构的即可.

(Ⅲ) 型群也可分为三组:

Ⅲ $\mathrm{A}(n>m\geqslant s;a,b,c)=\langle a,b,c \mid a^{p^n}=x, b^{p^m}=y, c^{p^s}=1, [a,b]=y, [a,c]=1, [b,c]=x, x^p=y^p=1, x,y\in Z(G)\rangle$, 其中 $n>m\geqslant s$.

Ⅲ $\mathrm{B}(m\geqslant n\geqslant s;a,b,c)=\langle a,b,c \mid a^{p^n}=x, b^{p^m}=y, c^{p^s}=1, [a,b]=y, [a,c]=1, [b,c]=x, x^p=y^p=1, x,y\in Z(G)\rangle$, 其中 $m\geqslant n\geqslant s$.

Ⅲ $\mathrm{C}(m\geqslant s>n;a,b,c)=\langle a,b,c \mid a^{p^n}=x, b^{p^m}=y, c^{p^s}=1, [a,b]=y, [a,c]=1, [b,c]=x, x^p=y^p=1, x,y\in Z(G)\rangle$, 其中 $m\geqslant s>n$.

令 p^u 为 G/G' 的型不变量中最小的数, 由 $|\mho_u(G)\bigcap G'|$ 知 Ⅱ A, Ⅲ C 间, Ⅱ B, Ⅲ C 间, Ⅱ C, Ⅲ A 间, Ⅱ C, Ⅲ B 间都互不同构. 所以只需判断 Ⅱ A, Ⅲ A 间, Ⅱ A, Ⅲ B 间, Ⅱ B, Ⅲ A 间, Ⅱ B, Ⅲ B 间及 Ⅱ C, Ⅲ C 之间的同构问题. 证明细节留给读者. □

定理 11.13.5　设 G 是三元生成的有限 p 群. 若 $c(G)=2$ 且 $G'\cong \mathrm{C}_p\times\mathrm{C}_p$, 则 $G\in J$ 当且仅当 G 同构于引理 11.13.4 中列出的群之一.

证明　由引理 11.13.4 知我们只需证明必要性.

设 $G/G'=\langle aG'\rangle\times\langle bG'\rangle\times\langle cG'\rangle$, 其中

$$o(aG')=p^n,\quad o(bG')=p^m,\quad o(cG')=p^s,\quad |\mho_1(G)\bigcap G'|\leqslant p^2.$$

情形 1　$|\mho_1(G)\bigcap G'|=1$.

不妨设 $G=\langle a,b,c \mid a^{p^n}=b^{p^m}=c^{p^s}=1,[a,b]=y,[a,c]=x,[b,c]=x^ry^t,x^p=y^p=1,x,y\in Z(G)\rangle$, 其中 $0\leqslant r,t\leqslant p-1$. 由群的关系式知 $\langle x,y\rangle\leqslant\langle[a,G]\rangle$, 这样就与引理 11.13.3 矛盾.

情形 2 $|\mho_1(G)\bigcap G'|=p$.

设 $G=\langle a,b,c\rangle$, 其中 $a^{p^n}=x$, $x^p=1$ 且 $x\in G'$. 若 $b^{p^m}=x^i$, 其中 $(i,p)=1$, $n\geqslant m$ 时, 用 $ba^{-ip^{n-m}}$ 替换 b; $n<m$ 时, 用 b 替换 a, $a^ib^{-p^{m-n}}$ 替换 b. 总之可设 $\langle b\rangle\bigcap G'=1$. 同理可设 $\langle c\rangle\bigcap G'=1$. 这样就可设

$$a^{p^n}=x,\quad b^{p^m}=c^{p^s}=1,\quad x^p=1$$

且 $x\in G'$. 因为 $|G'|=p^2$, 故 $[b,c]$, $[a,b]$ 和 $[a,c]$ 中至少有一个不在 $\langle x\rangle$ 中. 下面再分三种情况来讨论.

(2a) $[b,c]\notin\langle x\rangle$.

不妨设 $G=\langle a,b,c \mid a^{p^n}=x,b^{p^m}=c^{p^s}=1,[a,b]=x^iy^j,[b,c]=y,[a,c]=x^ry^t,x^p=y^p=1,x,y\in Z(G)\rangle$, 其中 $0\leqslant i,j,r,t\leqslant p-1$. 因为 $[b,a],[b,c]\in\langle[b,G]\rangle$, 由引理 11.13.3 知 $i=0$. 同理由 $[c,a],[c,b]\in\langle[c,G]\rangle$ 知, $r=0$. 因此 $|G'|=p$, 与假设矛盾.

(2b) $[a,b]\notin\langle x\rangle$.

此时可设 $G=\langle a,b,c \mid a^{p^n}=x,b^{p^m}=c^{p^s}=1,[a,b]=y,[a,c]=x^iy^j,[b,c]=x^ky^l,x^p=y^p=1,x,y\in Z(G)\rangle$, 其中 $0\leqslant i,j,k,l\leqslant p-1$. 由 $G'\cong \mathrm{C}_p\times \mathrm{C}_p$ 知, i 和 k 至少有一个不为 0. 因为 $\langle b\rangle\bigcap G'=1$ 和 $[b,a],[b,c]\in\langle[b,G]\rangle$, 故由引理 11.13.3 得, $k=0$. 故 $i\neq 0$. 由 $\langle c\rangle\bigcap G'=1$ 和引理 11.13.3 知, $[b,c]=1$.

断言 $n\geqslant s$ 且 $n\geqslant m$: 若否, 如果 $n<s$, 则存在 ca 使得 $\langle ca\rangle\bigcap G'=1$ 且 $\langle[ca,b],[ca,c]\rangle=G'$, 与引理 11.13.3 矛盾. 故 $n\geqslant s$. 类似地, 由 $\langle ba\rangle\bigcap G'=1$ 可得 $n\geqslant m$.

现在 $G=\langle a,b,c \mid a^{p^n}=x,b^{p^m}=c^{p^s}=1,[a,b]=y,[a,c]=x^iy^j,[b,c]=1,x^p=y^p=1,x,y\in Z(G)\rangle$, 其中 $1\leqslant i\leqslant p-1$, $0\leqslant j\leqslant p-1$, $n\geqslant s$ 并且 $n\geqslant m$.

若 $j=0$, 令 $c_1=c^{i^{-1}}$. 则

$$c_1^{p^s}=1,\quad [a,c_1]=[a,c^{i^{-1}}]=[a,c]^{i^{-1}}=x^{ii^{-1}}=x,$$

$$[b,c_1]=[b,c^{i^{-1}}]=[b,c]^{i^{-1}}=1.$$

用 c 代替 c_1 就可知 G 是 (Ⅰ) 型群.

若 $j\neq 0$ 且 $m\leqslant s$, 令 $c_1=cb^{-j}$. 则

$$c_1^{p^s}=1,\quad [a,c_1]=[a,cb^{-j}]=[a,c][a,b]^{-j}=x^iy^jy^{-j}=x^i,$$

$$[b, c_1] = [b, cb^j] = 1.$$

这种情形可化归为已经讨论过的 $j = 0$ 的情形. 若 $j \neq 0$ 且 $m > s$, 令

$$a_1 = a, \quad b_1 = c^{i^{-1}}, \quad c_1 = c^{i^{-1}} b^{-ji^{-1}}$$

和 $y_1 = xy^{ji^{-1}}$. 则

$$a_1^{p^n} = b_1^{p^s} = c_1^{p^m} = 1, \quad [a_1, b_1] = [a, c^{i^{-1}}] = [a, c]^{i^{-1}} = (x^i y^j)^{i^{-1}} = xy^{ji^{-1}} = y_1,$$

$$[a_1, c_1] = [a, c^{i^{-1}} b^{-ji^{-1}}] = [a, c]^{i^{-1}} [a, b]^{-ji^{-1}} = (x^i y^j)^{i^{-1}} y^{-ji^{-1}} = x,$$

$$[b_1, c_1] = [c^{i^{-1}}, c^{i^{-1}} b^{-ji^{-1}}] = 1.$$

这样 G 就化为 (I) 型群.

(2c) $[a, c] \notin \langle x \rangle$.

不妨设 $[a, b] = y$ 和 $G' = \langle x, y \rangle$. 互换 b, c 位置, 可化为情形 (2b).

情形 3　$|\mho_1(G) \bigcap G'| = p^2$.

不妨设 $G = \langle a, b, c \mid a^{p^n} = x, b^{p^m} = y, c^{p^s} = 1, [a, b] = x^i y^j, [b, c] = x^k y^l, [a, c] = x^r y^t, x^p = y^p = 1, x, y \in Z(G) \rangle$, 其中 $0 \leqslant i, j, k, l, r, t \leqslant p - 1$. 分 $[a, c] = 1$ 和 $[a, c] \neq 1$ 两种情况进行讨论.

(3a) $[a, c] = 1$.

因 $|G'| = p^2$, 故 $il - jk$ 不能被 p 整除. 由 $[cb, a], [cb, c] \in \langle [cb, G] \rangle$ 和引理 11.13.3 知 $m \geqslant s$.

下面分两种情况讨论: $l = 0$ 和 $l \neq 0$.

(3a.1) $l = 0$.

若 $n \geqslant s$, 令 $a_1 = a^{j^{-1}} c^{ij^{-1}k^{-1}}$, $b_1 = b$, $c_1 = c^{j^{-1}k^{-1}}$, $x_1 = x^{j^{-1}}$, 则 $[a_1, c_1] = 1$, 且

$$a_1^{p^n} = x^{j^{-1}} = x_1, \quad b_1^{p^m} = y, \quad c_1^{p^s} = 1,$$

$$[a_1, b_1] = [a^{j^{-1}} c^{ij^{-1}k^{-1}}, b] = (x^i y^j)^{j^{-1}} (x^k)^{-ij^{-1}k^{-1}} = y,$$

$$[b_1, c_1] = (x^k)^{j^{-1}k^{-1}} = x^{j^{-1}} = x_1.$$

从而 G 是 (III) 型群. 当 $s > n$ 且 $i = 0$ 时, 令 $a_1 = a^{j^{-1}}$, $b_1 = b$, $c_1 = c^{j^{-1}k^{-1}}$. 则 G 也是 (III) 型群. 若 $s > n$ 且 $i \neq 0$, 令

$$a_1 = a^i b^{jp^{m-n}}, \quad b_1 = b^{i^{-1}}, \quad c_1 = a^{-j^{-1}} c^{-j^{-1}k^{-1}i},$$

则 G 是 (II) 型群.

(3a.2) $l \neq 0$.

在此种情形下, 再分 $j=0$ 和 $j\neq 0$ 两种子情形讨论, 仍可得 G 为 (II) 型群或 (III) 型群. 细节略去. 总之, 当 $|\mho_1(G)\bigcap G'|=p^2$ 时, G 是 (II) 型群或 (III) 型群. □

11.13.2 类 2 的素数幂阶 J 群

在 11.13.1 节的基础上, 我们将分类幂零类为 2 的 J 群. 首先证明以下两个引理.

引理 11.13.6 *设 G 为有限非交换 p 群且为 J 群, $c(G)=2, G'\cong \mathrm{C}_p\times \mathrm{C}_p$. 则存在 $a_1,a_2,a_3,\cdots,a_r\in G$ 满足*

(a) $G/G'=\langle a_1G'\rangle\times\langle a_2G'\rangle\times\cdots\times\langle a_rG'\rangle$, *其中* $o(a_iG')=p^{m_i}$, $i=1,2,\cdots,r$ *并且* $m_1\geqslant m_2\geqslant\cdots\geqslant m_r$;

(b) $\langle a_1,a_2,a_3\rangle'=G'$.

证明 设 $G/G'=\langle a_1G'\rangle\times\langle a_2G'\rangle\times\cdots\times\langle a_rG'\rangle$, 其中 $o(a_iG')=p^{m_i}, i=1,2,\cdots,r, m_1\geqslant m_2\geqslant\cdots\geqslant m_r$. 当 $m_1=1$ 时, 由引理 11.5.9 直接可得结论. 下面讨论 $m_1>1$ 的情形.

设 i 是使 a_i 不在 $Z(G)$ 中的最小的正整数, 即存在 $j>i$ 使 $[a_i,a_j]\neq 1$. 若 $i\neq 1$, 说明 a_1 在 $Z(G)$ 中, 从而 $[a_1a_j,a_i]\neq 1$, 此时用 a_1a_j 替换 a_1, 仍然有其他关系成立. 不妨设 $i=1$, 即 $a_1\notin Z(G)$.

再设 j 是使 $[a_1,a_j]\neq 1$ 的最小的正整数. 若 $j\neq 2$, 说明 $[a_1,a_2]=1$, 从而 $[a_1,a_2a_j]\neq 1$, 此时用 a_2a_j 替换 a_2, 仍然有上面的关系成立. 不妨设 $j=2$, 即 $[a_1,a_2]\neq 1$.

再设 k 是使 $[a_k,a_l]\notin\langle[a_1,a_2]\rangle$ 的最小正整数. 若 $k>2$, 说明对所有的 s 都有 $[a_1,a_s]\in\langle[a_1,a_2]\rangle, [a_2,a_s]\in\langle[a_1,a_2]\rangle$.

(1) 若 $[a_1,a_l]=1$, 则

$$[a_1,a_2a_l]=[a_1,a_2],\quad [a_2a_l,a_k]=[a_2,a_k][a_l,a_k]\notin\langle[a_1,a_2]\rangle.$$

此时用 a_2a_l 替换 a_2, 仍然有其他关系成立. 不妨设 $k\leqslant 2$.

(2) 若 $[a_1,a_l]=[a_1,a_2]^u$, 其中 $(u,p)=1$, 再设 $[a_1,a_k]=[a_1,a_2]^v$, 则

$$[a_1,a_ka_l^{u^{-1}v}]=1,\quad [a_1,a_2a_ka_l^{u^{-1}v}]=[a_1,a_2],$$

$$[a_2a_ka_l^{u^{-1}v},a_l]=[a_2,a_l][a_k,a_l]\notin\langle[a_1,a_2]\rangle,$$

此时用 $a_2a_ka_l^{u^{-1}v}$ 替换 a_2, 仍然有其他关系成立. 不妨设 $k\leqslant 2$.

再设 l 是使 $[a_k,a_l]\notin\langle[a_1,a_2]\rangle$ 的最小正整数. 若 $l\neq 3$, 说明 $[a_1,a_3]\in\langle[a_1,a_2]\rangle$, $[a_2,a_3]\in\langle[a_1,a_2]\rangle$, 从而

$$[a_k,a_3a_l]=[a_k,a_3][a_k,a_l]\notin\langle[a_1,a_2]\rangle,$$

此时用 a_3a_l 替换 a_3, 仍然有其他关系成立. 不妨设 $l=3$.

综上可知, 经替换以后的 $a_1, a_2, a_3, \cdots, a_r$ 满足引理要求. □

下面给出有限 p 群不是 J 群的一个充分条件.

引理 11.13.7 设 G 为类 2 的有限 p 群, $G' \cong \mathrm{C}_p \times \mathrm{C}_p$. 若存在元素 $a, b, c, d \in G$ 满足 $G' = \langle [a,b], [c,d] \rangle$, $\langle a \rangle \bigcap G' = 1$, $\langle b \rangle \bigcap G' = 1$ 和 $\langle c \rangle \bigcap G' = 1$, 则 $G \notin J$.

证明 由假设和引理 11.13.3 知, $[b,c] \in \langle [a,b] \rangle$ 和 $[b,c] \in \langle [c,d] \rangle$. 因此 $[b,c]=1$. 因为 $\langle a \rangle \bigcap G' = 1$, 故 $[a,d] \in \langle [a,b] \rangle$. 因 $c(G)=2$ 和 $G' \cong \mathrm{C}_p \times \mathrm{C}_p$, 故 $G' = \langle [ac,b], [ac,d] \rangle$. 又 $\langle a \rangle \bigcap G' = 1$ 和 $\langle c \rangle \bigcap G' = 1$, 故 $\langle ac \rangle \bigcap G' = 1$. 从而由引理 11.13.3 得出 G 不是 J 群. □

定理 11.13.8 设 G 是有限 p 群. 若 $c(G)=2$, $G' \cong \mathrm{C}_p \times \mathrm{C}_p$, 则 $G \in J$ 当且仅当 G 同构于下列群之一.

(Ⅰ) $G = KM$, 其中 K 为 (Ⅰ) 型群, $M'=1$, $\exp(M) \leqslant p^n$ 且 $[K,M]=1$;

(Ⅱ) $G = KM$, 其中 K 为 (Ⅱ) 型群, $M'=1$, $\exp(M) \leqslant p^s$, $[M,a]=[M,c]=1$, $[M,y]=1$, $[M,b] \leqslant \langle x \rangle$;

(Ⅲ) $G = KM$, 其中 K 为 $n \geqslant s$ 时的 (Ⅱ) 型群, $M' \leqslant \langle y \rangle$, $\exp(M) \leqslant p^s$, $[M,x]=[M,y]=1$, $[M,K] \leqslant \langle y \rangle$;

(Ⅳ) $G = KM$, 其中 K 为 (Ⅲ) 型群, $M'=1$, $\exp(M) \leqslant p^s$, $[M,a]=[M,c]=1$, $[M,y]=1$, $[M,b] \leqslant \langle y \rangle$;

(Ⅴ) $G = KM$, 其中 K 为 $n \geqslant s$ 时的 (Ⅲ) 型群, $M' \leqslant \langle x \rangle$, $\exp(M) \leqslant p^s$, $[M,x]=[M,y]=1$, $[M,K] \leqslant \langle x \rangle$.

证明 首先证明定理中的群都是 J 群.

设 G 是 (Ⅰ) 型群. 若 $g \in G$ 且满足 $\langle g \rangle \bigcap G' = 1$, 则 $g = a^{ip}b^jc^ky^lm$, 其中 $m \in M$, i,j,k,l 都是非负整数. 由 $c(G)=2$ 和 $\exp(G')=p$ 知

$$[a^{ip}b^jc^ky^lm, b] = [a^{ip}b^jc^ky^lm, c] = [a^{ip}b^jc^ky^lm, M] = 1,$$

且

$$|[a^{ip}b^jc^ky^lm, G]| = |\langle [a^{ip}b^jc^ky^lm, a] \rangle| \leqslant p.$$

由引理 11.13.3 得 (Ⅰ) 型群是 J 群. 类似可证 (Ⅱ), (Ⅲ), (Ⅳ) 和 (Ⅴ) 型群都是 J 群.

下证必要性. 由引理 11.13.6, 不妨设 $G/G' = \langle a_1G' \rangle \times \langle a_2G' \rangle \times \cdots \times \langle a_rG' \rangle$, $o(a_iG') = p^{m_i}$ $(i=1,2,\cdots,r)$, 其中 $m_1 \geqslant m_2 \geqslant \cdots \geqslant m_r$ 且 $\langle a_1, a_2, a_3 \rangle$ 是引理 11.13.4 中列出的群之一. 进一步 $G = \langle a_1, a_2, \cdots, a_r \rangle$. 若 $r=3$, 由定理 11.13.5 可知, G 是定理中的群之一 (取 $M=1$ 即可).

现在假设 $r \geqslant 4$. 令 $K = \langle a_1, a_2, a_3 \rangle = \langle a, b, c \rangle$. 我们将构造子群 $M \leqslant G$ 使得 G 是定理中的群. 下面按照 K 的不同类型分三种情形进行讨论.

情形 1 $K=\langle a,b,c \mid a^{p^n}=x, b^{p^m}=c^{p^s}=1, [a,b]=y, [a,c]=x, [b,c]=1, x^p=y^p=1, x,y\in Z(G)\rangle$, 其中 $n\geqslant s$, $n\geqslant m$.

设 j 是大于 3 的满足 $a_j^{p^{m_j}}=x^uy^v, (v,p)=1$ 的最小正整数. 用 $(a_ja^{-up^{n-m_j}})^{v^{-1}}$ 替换 a_j, 不妨设 $a_j^{p^{m_j}}=y$.

当 $k\geqslant 4$ 且 $k\neq j$ 时, 可设 $a_k^{p^{m_k}}=1$. 事实上, 若 $j>k\geqslant 4$, 则 $a_k^{p^{m_k}}=x^u$. 用 $a_ka^{-up^{n-m_k}}$ 替换 a_k, 可设 $a_k^{p^{m_k}}=1$. 若 $k>j$, 则 $a_k^{p^{m_k}}=x^uy^v$ $(u\geqslant 0, v\geqslant 0)$. 用 $a_ka^{-up^{n-m_k}}a_j^{-vp^{m_j-m_k}}$ 替换 a_k, 可得 $a_k^{p^{m_k}}=1$. 因此 $\langle a_k\rangle\bigcap G'=1$. 若 $[a_k,a]=x^uy^v$, 则用 $a_kb^vc^u$ 替换 a_k. 从而可设 $[a_k,a]=1$, $\langle a_k\rangle\bigcap G'=1$ 且 $o(a_k)\leqslant p^n$. 断言: $[a_k,b]=[a_k,c]=1$. 若 $[a_k,b]\neq 1$, 则由引理 11.13.3 知, $[a_k,b]=y^u$, 其中 $(u,p)=1$. 注意到 $[a,c]=x$, 由引理 11.13.7 得 G 不是 J 群, 矛盾. 所以 $[a_k,b]=1$. 同理可证 $[a_k,c]=1$.

令 $N=\langle\{a_k \mid k\neq j, k\geqslant 4\}\rangle$. 因为 $[a,c]=x$ 且 $[a,b]=y$, 由引理 11.13.7 知 N 交换. 进一步有 $G=KN\langle a_j\rangle$, 其中 $\exp(N)\leqslant p^n$, $[K,N]=1$, $N\bigcap G'=1$, $a_j^{p^{m_j}}=y$ 和 $m_j\leqslant\min\{m,s\}$. 下面分两种情形讨论: (1a) $s=m=m_j$ 和 (1b) $\max\{m,s\}>m_j$ 且 $\min\{m,s\}\geqslant m_j$.

(1a) $s=m=m_j$.

设 $[a_j,a]=x^uy^v$. 令 $e=a_jb^vc^u$. 则 $[e,a]=1$, $e^{p^{m_j}}=y$ 且 $G=KN\langle e\rangle$.

(1a.1) $[e,b]=1$.

因 $[bc,e]=[c,e]$, $[bc,a]=y^{-1}x^{-1}$ 和 $[c,a]=x^{-1}$, 故由引理 11.13.3 知,

$$[e,c]\in\langle y^{-1}x^{-1}\rangle\bigcap\langle x^{-1}\rangle=1.$$

因此 $[e,K]=1$. 对任意的 $g\in N$, 注意到

$$[bg,e]=[g,e],\quad [bg,a]=y^{-1},\quad [cg,e]=[g,e],\quad [cg,a]=x^{-1}.$$

由引理 11.13.3 得 $[e,g]\in\langle y\rangle\bigcap\langle x\rangle=1$. 于是 $[e,N]=1$. 令 $M=\langle N,e\rangle$. 则得定理中的 (I) 型群.

(1a.2) $[e,b]\neq 1$.

可设 $[e,b]=y$. 由 $[bc,e]=y^{-1}[c,e]$, $[bc,a]=y^{-1}x^{-1}$, $[a,c]=x$ 和引理 11.13.3 得 $[e,c]=x$. 注意到 $o(aG')=o(acG')$ 且 $o(eG')=o(cG')$. 令 $\{a_1,a_2,a_3\}=\{ac,b,e\}$. 则转化为下面将会讨论的情形 (2) 和 (3).

(1b) $\max\{m,s\}>m_j$ 且 $\min\{m,s\}\geqslant m_j$.

类似于情形 (1a) 的讨论, 也可得 G 为定理中的 (I) 型群. 细节略去.

情形 2 $K=\langle a,b,c \mid a^{p^n}=x, b^{p^m}=y, c^{p^s}=1, [a,b]=x, [a,c]=1, [b,c]=y, x^p=y^p=1, x,y\in Z(G)\rangle$, 其中 $m\geqslant s$.

当 $i \geqslant 4$ 时, 设 $a_i^{p^{m_i}} = x^{u_i}y^{v_i}$. 用 $a_i a^{-u_i p^{n-m_i}} b^{-v_i p^{m-m_i}}$ 替换 a_i, 不妨设 $a_i^{p^{m_i}} = 1$.

若 $[a_i, c] \neq 1$, 则由引理 11.13.3 可设 $[a_i, c] = y$. 进而 $[a_i, a], [a_i, b] \in \langle y \rangle$.

当 $[a_i, c] = 1$ 且 $[a_i, a] = 1$ 时, 设 $[a_i, b] = x^k y^j$. 若 $(k, p) = 1$, 则用 $a_i^{k^{-1}} c^{jk^{-1}}$ 替换 a_i 可得 $[a_i, b] = x$ 和 $o(a_i) \leqslant p^s$. 若 $p|k$, 用 $a_i c^j$ 替换 a_i, 从而可设 $[a_i, b] = 1$ 和 $o(a_i) \leqslant p^s$.

若 $[a_i, c] = 1$ 且 $[a_i, a] \neq 1$, 则由引理 11.13.3 得

$$[a_i, b] \in \langle [a_i, a] \rangle, \quad [a_i, b]y^{-1} = [a_i c, b] \in \langle [a_i c, a] \rangle = \langle [a_i, a] \rangle.$$

所以 $y \in \langle [a_i, a] \rangle$. 进而可设 $[a_i, a] = y$ 和 $[a_i, c], [a_i, b] \in \langle y \rangle$.

现在 $G = K\langle \{a_i \mid i \geqslant 4\} \rangle$, $o(a_i) \leqslant p^s$ 且 $\langle a_i \rangle \bigcap G' = 1$. a_i 和 K 的关系只能是下列四种关系之一.

(a) $[a_i, c] = y$, $[a_i, a], [a_i, b] \in \langle y \rangle$;

(b) $[a_i, c] = 1$, $[a_i, a] = 1$, $[a_i, b] = 1$;

(c) $[a_i, c] = 1$, $[a_i, a] = 1$, $[a_i, b] = x$;

(d) $[a_i, c] = 1$, $[a_i, a] = y$, $[a_i, b] \in \langle y \rangle$.

令

$$R_1 = \{a_i \mid i \geqslant 4, \ \ [a_i, c] = y, \ \ [a_i, a], [a_i, b] \in \langle y \rangle\};$$
$$R_2 = \{a_i \mid i \geqslant 4, \ \ [a_i, c] = 1, \ \ [a_i, a] = 1, \ \ [a_i, b] = 1\};$$
$$R_3 = \{a_i \mid i \geqslant 4, \ \ [a_i, c] = 1, \ \ [a_i, a] = 1, \ \ [a_i, b] = x\};$$
$$R_4 = \{a_i \mid i \geqslant 4, \ \ [a_i, c] = 1, \ \ [a_i, a] = y, \ \ [a_i, b] \in \langle y \rangle\}.$$

下面我们分两种情形讨论: (2a)$R_3 \neq \varnothing$ 和 (2b)$R_3 = \varnothing$.

(2a) $R_3 \neq \varnothing$.

此时存在 a_i $(i \geqslant 4)$ 满足 $[a_i, b] = x$. 若存在 a_v $(v \geqslant 4)$ 满足 $[a_v, c] = y$, 则 $G' = \langle [a_i, b], [a_v, c] \rangle$. 由引理 11.13.7 得 G 不是 J 群, 矛盾. 所以 $R_1 = \varnothing$. 由引理 11.13.3 知, $R_4 = \varnothing$. 注意到 $[b, c] = y$ 和 $[a_i, b] = x$. 由引理 11.13.7 知,

$$[\langle R_2 \rangle, \langle R_3 \rangle] = \langle R_2 \rangle' = \langle R_3 \rangle' = 1.$$

令 $M = \langle \{a_i | i \geqslant 4\} \rangle$. 我们有

$$G = KM, \quad M' = 1, \quad [M, a] = [M, c] = 1, \quad \langle [M, b] \rangle = \langle x \rangle, \quad \exp(M) \leqslant p^s,$$

即得 G 是定理中的 (II) 型群.

(2b) $R_3 = \varnothing$. 令 $M = \langle \{a_i | i \geqslant 4\} \rangle$.

(2b.1) $n \geqslant s$.

易知 $G = KM$, $M' \leqslant \langle y \rangle$, $[M, K] \leqslant \langle y \rangle$ 和 $\exp(M) \leqslant p^s$. 从而得到了定理中的 (III) 型群.

(2b.2) $n < s$.

首先断言 $R_1 = \varnothing$. 若 $R_1 \neq \varnothing$, 则存在整数 u, v 和元素 a_i 满足 $(vu, p) = 1$ 和 $[ac^v, a_i] = y^u$. 由 $[ac^v, b] = xy^{-v}$ 知, $\langle [ac^v, G] \rangle = G'$. 从而与引理 11.13.3 矛盾. 然后还断言 $R_4 = \varnothing$. 若否, 存在 a_i 满足 $[ac, a_i] = y^{-1}$. 注意到 $[ac, b] = xy^{-1}$. 由引理 11.13.3 可得矛盾. 最后断言 $M' = 1$. 若 $M' \neq 1$, 则存在 m_1 和 m_2 满足 $[m_1, m_2] \neq 1$. 因 $[b, c] = y$, 由引理 11.13.7 得, $[m_1, m_2] = y^w$ $((w, p) = 1)$. 因

$$[acm_1, m_2] = y^w, \quad [acm_1, b] = xy^{-1},$$

我们知 $\langle [acm_1, G] \rangle = G'$, 与引理 11.13.3 矛盾, 即得 G 是定理中的 (II) 型群.

情形 3 $K = \langle a, b, c \mid a^{p^n} = x, b^{p^m} = y, c^{p^s} = 1, [a, b] = y, [a, c] = 1, [b, c] = x, x^p = y^p = 1, x, y \in Z(G) \rangle$, 其中 $m \geqslant s$.

用情形 2 中类似的证明可得定理中的 (IV) 和 (V) 型群. □

第 12 章　有限亚 Hamilton p 群

众所周知, 正规子群与交换子群是群论中两类基本的子群. 它们在群论研究中的地位举足轻重. 在 p 群研究领域中, 内交换 p 群和 Hamilton p 群的分类是两个经典的结果. 内交换 p 群可看作交换性 "最强" 的非交换群. 而 Hamilton p 群则可看作正规性 "最强" 的非交换群. 就像我们在前几章看到的, 沿着这两个方向, 国内外许多群论学者分别对交换性 "较强" 的 p 群以及正规性 "较强" 的 p 群做了大量的研究, 取得了丰富的成果. 而亚 Hamilton p 群作为这两个经典结果的推广, 既可看作交换性 "较强", 也可看作正规性 "较强" 的非交换群. 所谓亚 Hamilton p 群, 就是子群或交换或正规的非交换 p 群. 换句话说, 亚 Hamilton p 群就是非交换子群均正规的群, 也可以说, 非正规子群均交换的群. 容易看出, Dedekind[57] 分类的 Dedekind p 群、Rédei[192] 分类的内交换 p 群、Passman[181] 分类的非正规子群均循环的 p 群、Berkovich 和 Janko[27] 与张勤海等 [273] 分类的 $\mathcal{A}_2$ 群, 以及张勤海等 [275] 分类的非正规子群的阶不超过 p^2 的 p 群等均是亚 Hamilton p 群. 因而 Hamilton p 群是有限 p 群中比较大的群类.

20 世纪 60~70 年代, Nagrebeckǐ 在文献 [165]—[167] 中, 对于亚 Hamilton 群已经做了许多工作. 例如, Nagrebeckǐ 在 [166] 中证明了下面的定理.

定理 12.0.1　*设 G 是有限非幂零群, 则 G 是亚 Hamilton 群当且仅当 $G = SZ(G)$, 其中 S 是下列群之一:*

(1) $S = P \rtimes Q$, *其中 P 是初等交换 p 群, Q 循环并且 $(p, |Q|) = 1$;*

(2) $S = P \rtimes Q$, *其中 $P \cong Q_8$ 且 Q 是奇阶循环群;*

(3) $S = P \rtimes Q$, *其中 $|P| = p^3, p \geqslant 5$, Q 循环并且 $(p, |Q|) = 1$.*

由此可知, 研究幂零的亚 Hamilton 群的问题本质上可归结为研究亚 Hamilton p 群的问题. 而它们的结构远比非幂零的情况复杂得多. 安立坚在他的博士论文 [3] 中开始了对亚 Hamilton p 群的研究, 证明了亚 Hamilton p 群一定是亚交换的. 给出了其分类, 并彻底解决了同构问题, 从而完整地解决了亚 Hamilton 群的同构分类问题. 也见文献 [10],[61]. 本章介绍这项成果. 证明与文献 [3] 的原始证明有所不同.

12.1　亚 Hamilton p 群的性质

首先给出几个简单的引理.

引理 12.1.1 设 G 是有限亚 Hamilton 群. 则 G 的截断也是亚 Hamilton 群.

定义 12.1.2 称群 G 满足 n-Engel **条件**, 如果对任意的 $g, h \in G$, 有

$$[g, \underbrace{h, \cdots, h}_{n}] = 1.$$

定理 12.1.3 设群 G 满足 2-Engel条件, 则 G 是幂零类至多为 3 的幂零群. 如果 G 中没有 3 阶元素, 则 $c(G) \leqslant 2$.

引理 12.1.4 设 G 是有限亚 Hamilton p 群, $x \in G$. 则 x 的正规闭包 $\langle x\rangle^G$ 是交换群或者内交换群.

证明 若 $\langle x\rangle^G$ 不交换, 则存在 $g \in G$ 使得 $[x, x^g] \neq 1$. 由定义, $K := \langle x, x^g\rangle \trianglelefteq G$. 于是 $K = \langle x\rangle^G$. 令 $y = x^g$. 因为 $\langle x, x^y\rangle$ 是 K 的真子群, 若 $[x, x^y] \neq 1$, 则亦有 $\langle x, x^y\rangle = \langle x\rangle^G = K$, 矛盾. 所以, 我们有 $[x, x^y] = 1$. 由此得 $[x, y, x] = 1$. 交换 x 和 y 的位置, 又可得 $[x, y, y] = 1$. 于是 $c(K) = 2$.

再考虑 K 的真子群 $\langle x, y^p\rangle$. 同样的道理可得 $[x, y^p] = 1$. 因 $c(K) = 2$, 有 $[x, y]^p = 1$. 这推出 $K' = \langle [x, y]\rangle$ 是 p 阶群. 由定理 1.7.7 得 K 内交换. □

定理 12.1.5 设 G 是有限 p 群. 则 G 是亚 Hamilton 群当且仅当它的每个二元生成的非交换子群都正规.

证明 必要性显然. 只需证明充分性.

用反证法. 假设 G 不是亚 Hamilton 群, 则 G 中存在不正规的非交换子群. 设 H 是阶最小的 G 的不正规的非交换子群. 由题设 H 不是二元生成的, 从而 H 至少有 $1 + p + p^2$ 个极大子群. 再由引理 1.7.1 可知, H 至少有两个非交换的极大子群 N_1 和 N_2. 由 H 的极小性, N_1 和 N_2 都是 G 的正规子群. 从而 $H = N_1N_2$ 也是 G 的正规子群, 矛盾. □

定理 12.1.6 有限亚 Hamilton p 群 G 的幂零类至多为 3. 特别地, G 亚交换.

证明 由引理 12.1.4, 任何元素 x 的正规闭包 $K = \langle x^g\rangle$ 若不交换, 则内交换. 在 K 内交换的情况下, K' 作为 K 的特征子群, 是 G 的阶为 p 的正规子群. 于是 $K' \leqslant Z(G)$. 这样, $G/Z(G)$ 中任何元素之正规闭包均交换, 从而 $G/Z(G)$ 满足 2-Engel 条件. 由定理 12.1.3, 只要 $p \neq 3$, 就有 $c(G) \leqslant 3$; 而若 $p = 3$, 有 $c(G) \leqslant 4$.

现在假定 $p = 3$. 下证 $c(G) \leqslant 3$. 设 G 是极小阶反例, 则由引理 12.1.1 可知 $c(G) = 4$, $|G_4| = p$, 并且 G 的每个真子群和真商群的幂零类至多为 3. 于是可设 $G_4 = \langle [a, b, c, d]\rangle$, $a, b, c, d \in G$. 还不妨设 $a, b, c, d \notin \Phi(G)$. 记 $x = [a, b, c]$, 则 $N = \langle x, d\rangle$ 为内交换群. 从而 $N \trianglelefteq G$, 并由定理条件, 包含 N 的子群皆在 G 中正规. 这得到 G/N 为 Dedekind 群. 因为 $p = 3$, G/N 交换. 又由 $d \notin \Phi(G)$ 知 $G' \leqslant N \bigcap \Phi(G) < N$, 从而 G' 交换. 于是 $[[c, d], [a, b]] = 1$. 又由 $[a, b] \in N$ 和

$d \in N$, 知 $[d,[a,b]] \in N' \leqslant Z(G)$, 从而 $[d,[a,b],c]=1$. 最后应用命题 1.1.8(4) 可得 $[[a,b],c,d]=1$, 矛盾. □

定理 12.1.7 设 G 是有限 p 群. 则 G 是亚 Hamilton 群当且仅当 G' 包含在 G 的每个非交换子群之中.

证明 充分性显然, 下面证明必要性.

设 G 是极小阶的反例. 则 G 中存在内交换子群 $N=\langle a,b\rangle$ 使得 $G' \not\leqslant N$. 由于 G 为亚 Hamilton 群, G 的包含 N 的子群全都正规, 从而 G/N 为 Hamilton 群. 由 G 的极小性, $G/N \cong \mathrm{Q}_8$. 令 $G/N=\langle xN,yN\rangle$, $H=\langle x,y\rangle$. 则

$$G=HN, \quad H/(H\bigcap N)\cong \mathrm{Q}_8,$$

$$z:=[x,y]\notin N,\ H\bigcap N \leqslant \Phi(H) \quad 且 \quad H\bigcap N=\langle x^4,x^2y^2,x^2[x,y]\rangle^H.$$

易知 $z \in \langle x\rangle^H$. 由引理 12.1.4 可知, $\langle z,x\rangle$ 交换或内交换, 从而一定有 $[z,x]^2=[z,x]^2=1$. 同理 $[z,y^2]=[z,y]^2=1$. 这首先说明 $\exp(H_3)\leqslant 2$. 又因为 $\Phi(H)=\langle x^2,y^2,H'\rangle$, 以及 H' 交换 (定理 12.1.6), 可得 $[\Phi(H),z]=1$. 特别地, $[H\bigcap N,z]=1$. 下面分五种情形推出矛盾.

(1) $H\bigcap N=N$.

此时 $[N,z]=1$. 设 $M=\langle za,b\rangle$, 则由定理 1.7.7 可知 M 为内交换群, 从而 G/M 也是 Hamilton 群. 由于 $z\notin M$, G/M 非交换. 再由 G 的极小性可知 $H/M=G/M\cong \mathrm{Q}_8$. 故又有 $M=\langle x^4,x^2y^2,x^2[x,y]\rangle^H=N=\langle a,b\rangle$, 矛盾.

(2) $H\bigcap N<N$ 且 $H\bigcap N \not\leqslant \Phi(N)$.

此时, $H\bigcap N$ 包含 N 的一个生成元. 不妨设 N 的生成元 $a\in H\bigcap N, b\notin H\bigcap N$. 则 $[z,a]=1$. 因为 $H\bigcap N$ 交换, 所以 $[x^2y^2,x^2[x,y]]=1$, 进而 $[x^2,y^2]=1$. 计算可得

$$[x^2,y^2]=[x^2,y]^2=[x,y]^4=z^4.$$

若 $z^2\neq 1$, 则有 $\langle z^2\rangle=\mho_1(H')$ 为 G 的极小正规子群. 故总有 $z^2\in Z(G)$. 特别地, $[z,b]^2=[z^2,b]=1$.

(i) 若 $[z,b]\neq[a,b]$. 令 $M=\langle za,b\rangle$, 由定理 1.7.7 可知 M 为内交换群, 从而 G/M 也是 Hamilton 群. 由于 $z\notin M$, G/M 非交换. 再由 G 的极小性可知

$$G/M=HM\cong H/(H\bigcap M)\cong \mathrm{Q}_8.$$

故又有

$$H\bigcap M=\langle x^4,x^2y^2,x^2[x,y]\rangle^H=H\bigcap N.$$

从而 $a\in H\bigcap N=H\bigcap M\leqslant M$. 进一步有 $z=(za)a^{-1}\in M$, 矛盾.

(ii) 若 $[z,b]=[a,b]$, 则 $L:=\langle z,b\rangle\bigcap N$ 为 G 的包含 b 的正规子群. 令 K 为 N 的包含 L 的极大子群, 且 $K\trianglelefteq G$, 则 G/K 一定是二元生成的 2^4 阶群, 且它有商群与 Q_8 同构. 由 2^4 阶群的分类可知, $G/K=\langle xK,yK\rangle:=\langle\bar{x},\bar{y}\rangle\cong \mathrm{M}_2(2,2)$. 其定义关系为

$$\bar{x}^4=\bar{y}^4=1,\quad [\bar{x},\bar{y}]=\bar{x}^2.$$

易知, $\langle\bar{y}\rangle$ 和 $\langle\bar{x}\bar{y}\rangle$ 均为 G/K 的不正规的子群, 所以, 它们的完全反像也是 G 的不正规的子群, 从而是交换群. 由此有 $[y,K]=1$, $[xy,K]=1$, 进而 $[H,K]=1$. 这与 $[z,b]=[a,b]\neq 1$ 矛盾.

(3) $H\bigcap N<\Phi(N)$.

此时, 首先断言 $H\bigcap N\neq 1$: 若否, 则 $G=H\times N$. 因为 $N\cong G/H$ 一定是 Hamilton 群, 所以 $N\cong \mathrm{Q}_8$. 此时 $\langle xa,yb\rangle\cong\mathrm{Q}_8$ 在 G 中不正规, 矛盾.

还可以进一步断言 $N'\leqslant H\bigcap N$. 若否, 则 $G/(H\bigcap N)$ 也是反例, 与 G 的极小性矛盾. 令

$$\overline{G}=G/(H\bigcap N),\quad \overline{H}=H/(H\bigcap N)=\langle\bar{x},\bar{y}\rangle,\quad \overline{N}=N/(H\bigcap N)=\langle\bar{a}\rangle\times\langle\bar{b}\rangle.$$

则 $\overline{G}=\overline{H}\times\overline{N}$, 且 $\overline{N}$ 中必有阶不小于 4 的元素, 不妨设 $o(\bar{a})\geqslant 4$. 设 $\overline{K}=\langle\bar{x}\bar{a}\rangle\times\langle\bar{b}\rangle$, 则 $\overline{K}$ 在 $\overline{G}$ 中不正规, 所以它的完全反像在 G 中也都不正规, 从而是交换群. 这意味着 $[xa,b]=1$(即 $[x,b]=[a,b]$). 将 $\bar{x}$ 换为 $\bar{y}$ 或 $\bar{x}\bar{y}$ 后, 同理可得 $[y,b]=[a,b]$ 和 $[xy,b]=[a,b]$, 而这是不可能的.

(4) $H\bigcap N=\Phi(N)=N'$.

此时,

$$|N|=2^3,\quad |H|=2^4,\quad |G|=2^6,\quad G/N'=H/N'\times\langle aN'\rangle\times\langle bN'\rangle.$$

因为 $\langle aN'\rangle$ 和 $\langle bN'\rangle$ 在 G/N' 中正规, 所以它们的完全反像 $A:=\langle a,N'\rangle$ 和 $B:=\langle b,N'\rangle$ 在 G 中也正规. 注意到 A 和 B 均为 4 阶群, 由 N/C 定理可知, $C_G(A)$ 和 $C_G(B)$ 均为 G 的极大子群. 令 $K=C_G(A)\bigcap C_G(B)$, 则 $|K|\geqslant 2^4$. 因为 $K\bigcap N=Z(N)=N'$, 所以 $|KN|=(|K||N|)/|K\bigcap N|\geqslant 2^6$, 从而 $G=K*N$. 因为 $KN/N\cong K/K\bigcap N\cong\mathrm{Q}_8$, 不妨设 $H=K$. 由 2^4 阶群的分类可知, $H=\langle x,y\rangle\cong\mathrm{M}_2(2,2)$. 其定义关系为

$$x^4=y^4=1,\quad [x,y]=x^2$$

且 $N'=H\bigcap N=\langle x^2y^2\rangle$. 设 a 为 N 中的 4 阶元, 则 $a^2=x^2y^2$. 计算可知 $[x,ay]=x^2$, $(ay)^2=x^2$. 从而子群 $\langle x,ay\rangle$ 既不交换也不正规, 矛盾.

(5) $H\bigcap N=\Phi(N)\neq N'$.

令 K 为 $H\bigcap N$ 的极大子群, 且在 G 中正规. 首先断言 $N' \leqslant K$. 若否, 则 G/K 也是反例, 与 G 的极小性矛盾, 所以断言成立. 从而 N/K 为交换群. 设

$$\overline{G} = G/K, \quad \overline{H} = H/K = \langle \bar{x}, \bar{y} \rangle, \quad \overline{N} = N/K = \langle \bar{a} \rangle \times \langle \bar{b} \rangle,$$

其中 $o(\bar{a}) = 4$. 由 2^4 阶群的分类可知, $H/K \cong \mathrm{M}_2(2,2)$. 其定义关系为

$$\bar{x}^4 = \bar{y}^4 = 1, \quad [\bar{x}, \bar{y}] = \bar{x}^2$$

且 $\bar{a}^2 = \bar{x}^2\bar{y}^2$, $\Phi(N)/K = (H\bigcap N)/K = \langle \bar{x}^2\bar{y}^2 \rangle$. 我们有 $\bar{a} \notin Z(\overline{G})$ (若否, 则 $\langle \bar{x}, \bar{a}\bar{y} \rangle$ 在 $\overline{G}$ 中既不交换也不正规, 矛盾). 我们还有 $[\bar{a}, \bar{x}] \neq \bar{1}$(若否, 由 $\bar{a} \notin Z(\overline{G})$ 可得 $[\bar{a}, \bar{y}] = \bar{x}^2\bar{y}^2$, 从而 $\langle \bar{a}\bar{x}, \bar{y} \rangle$ 在 $\overline{G}$ 中既不交换也不正规, 矛盾). 所以必有 $[\bar{a}, \bar{x}] = \bar{x}^2\bar{y}^2$. 将上面的 $\bar{a}$ 换为 $\bar{a}\bar{b}$ 考虑, 同理可得 $[\bar{a}\bar{b}, \bar{x}] = \bar{x}^2\bar{y}^2$, 从而 $[\bar{b}, \bar{x}] = 1$. 我们又有 $[\bar{b}, \bar{y}] = \bar{1}$(若否, 则 $[\bar{b}, \bar{y}] = \bar{x}^2\bar{y}^2$. 计算可知 $\langle \bar{x}, \bar{b}\bar{y} \rangle$ 在 $\overline{G}$ 中既不交换也不正规, 矛盾).

现在, 容易看出 $\langle \bar{x}, \bar{b} \rangle$ 和 $\langle \bar{a}\bar{x}, \bar{b} \rangle$ 在 $\overline{G}$ 中均不正规, 所以它们的完全反像在 G 中也不正规, 从而交换. 所以 $[x, b] = 1$ 及 $[ax, b] = 1$, 这与 $[a, b] \neq 1$ 矛盾. □

下面讨论导群初等交换的亚 Hamilton p 群. 将证明这样的群当幂零类为 3 的时候是 $\mathcal{A}_2$ 群. 首先给出 $\mathcal{A}_2$ 群的一些结论. 它们由 $\mathcal{A}_2$ 群的分类直接可得.

引理 12.1.8　*设 G 为导群初等交换的 $\mathcal{A}_2$ 群, 且 $c(G) > 2$. 则 G 为以下互不同构的群之一.*

(1) p^4 阶的极大类 p 群 (p 为奇数).

(i) $\langle a, b, c, d \mid a^p = b^p = c^p = d^p = 1, [c, d] = b, [b, d] = a, [a, b] = [a, c] = [a, d] = [b, c] = 1 \rangle$;

(ii) $\langle a, b, c \mid a^{p^2} = b^p = 1, c^p = a^{\alpha p}, [a, b] = a^p, [a, c] = b, [b, c] = 1 \rangle$, 其中 $\alpha = 0, 1$ 或是一个模 p 的平方非剩余 (三种互不同构的群);

(iii) $p = 3$, $\langle a, b, c \mid a^9 = b^3 = c^3 = 1, [a, b] = 1, [a, c] = b, [c, b^{-1}] = a^{-3} \rangle$.

(2) 二元生成有交换极大子群的 $\mathcal{A}_2$ 群 ($n \geqslant 5$, p 为奇数).

(i) $\langle b, a_1, a_2, a_3 \mid b^{p^{n-3}} = a_1^p = a_2^p = a_3^p = 1, [a_1, b] = a_2, [a_2, b] = a_3, [a_i, a_j] = 1, [a_3, b] = 1 \rangle$, 其中 $1 \leqslant i, j \leqslant 3$;

(ii) $\langle b, a_1, a_2 \mid b^{p^{n-2}} = a_1^p = a_2^p = 1, [a_1, b] = a_2, [a_2, b] = b^{p^{n-3}}, [a_1, a_2] = 1, [b^{p^{n-3}}, a_1] = [b^{p^{n-3}}, a_2] = 1 \rangle$;

(iii) $\langle b, a_1, a_2 \mid b^{p^{n-3}} = a_1^{p^2} = a_2^p = 1, [a_1, b] = a_2, [a_2, b] = a_1^{\nu p}, [a_1, a_2] = 1, [a_1^p, b] = [a_1^p, a_2] = 1 \rangle$, 其中 $\nu = 1$ 或者 ν 是一个固定的模 p 的平方非剩余.

(3) 无交换极大子群的 $\mathcal{A}_2$ 群 ($p \geqslant 5$).

(i) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = b^{\nu p}, [c, b] = a^p \rangle$, 其中 ν 是固定的模 p 的平方非剩余;

(ii) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=c,[c,a]=a^{-p}b^{-lp},[c,b]=a^{-p}\rangle$, 其中 $4l=g^{2r+1}-1$ 对于 $r=1,2,\cdots,\dfrac{1}{2}(p-1)$, g 是模 p 的最小原根;

(4) 无交换极大子群的 $\mathcal{A}_2$ 群 ($p=3$).

(i) $\langle a,b,c \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^3\rangle$;

(ii) $\langle a,b,c \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^{-3}\rangle$.

推论 12.1.9 设 G 为导群初等交换的 $\mathcal{A}_2$ 群, 且 $c(G)>2$. 则 $d(G)=2$ 且 p 为奇素数.

引理 12.1.10 设 G 是导群初等交换的亚 Hamilton p 群. 若 G 不是 $\mathcal{A}_2$ 群, 则 G 的 $\mathcal{A}_2$ 子群都是类 2 的.

证明 假设结论不成立, 则 G 中存在导群初等交换的类 3 的 $\mathcal{A}_2$ 子群 K. 由引理 12.1.8 可知, p 为奇素数且 K 只能是以下几种群之一.

(1) p^4 阶的极大类 p 群.

(i) $\langle a,b,c,d \mid a^p=b^p=c^p=d^p=1,[c,d]=b,[b,d]=a,[a,b]=[a,c]=[a,d]=[b,c]=1\rangle$;

(ii) $\langle a,b,c \mid a^{p^2}=b^p=1,c^p=a^{\alpha p},[a,b]=a^p,[a,c]=b,[b,c]=1\rangle$, 其中 $\alpha=0,1$ 或 α 是一个模 p 的平方非剩余 (三种互不同构的群);

(iii) $p=3$, $\langle a,b,c \mid a^9=b^3=c^3=1,[a,b]=1,[a,c]=b,[c,b^{-1}]=a^{-3}\rangle$.

(2) 二元生成有交换极大子群的 $\mathcal{A}_2$ 群 ($n\geqslant 5$).

(i) $\langle b,a_1,a_2,a_3 \mid b^{p^{n-3}}=a_1^p=a_2^p=a_3^p=1,[a_1,b]=a_2,[a_2,b]=a_3,[a_i,a_j]=1,[a_3,b]=1\rangle$, 其中 $1\leqslant i,j\leqslant 3$;

(ii) $\langle b,a_1,a_2 \mid b^{p^{n-2}}=a_1^p=a_2^p=1,[a_1,b]=a_2,[a_2,b]=b^{p^{n-3}},[a_1,a_2]=1,[b^{p^{n-3}},a_1]=[b^{p^{n-3}},a_2]=1\rangle$;

(iii) $\langle b,a_1,a_2 \mid b^{p^{n-3}}=a_1^{p^2}=a_2^p=1,[a_1,b]=a_2,[a_2,b]=a_1^{\nu p},[a_1,a_2]=1,[a_1^p,b]=[a_1^p,a_2]=1\rangle$, 其中 $\nu=1$ 或 ν 是一个固定的模 p 平方非剩余.

(3) 无交换极大子群的 $\mathcal{A}_2$ 群 ($p\geqslant 5$).

(i) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=c,[c,a]=b^{\nu p},[c,b]=a^p\rangle$, 其中 ν 是固定的模 p 的平方非剩余;

(ii) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=c,[c,a]=a^{-p}b^{-lp},[c,b]=a^{-p}\rangle$, 其中 $4l=g^{2r+1}-1$ 对于 $r=1,2,\cdots,\dfrac{1}{2}(p-1)$, g 是模 p 的最小原根.

(4) 无交换极大子群的 $\mathcal{A}_2$ 群 ($p=3$).

(i) $\langle a,b,c \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^3\rangle$;

(ii) $\langle a,b,c \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^{-3}\rangle$.

设 H 是 G 的以 K 为极大子群的子群, 然后分情况推出矛盾.

情形 1 K 为上面所列的 (2) 型群.

易知 $K/Z(K)$ 为 p^3 阶的非亚循环的内交换群. 则 $H/Z(K)$ 为非亚循环的 p^4 阶群. 若 $d(H/Z(K))=2$, 由 p^4 阶群的分类可知 $H/Z(K)$ 是极大类的. 从而

$$K'Z(K)/Z(K)=H_3Z(K)/Z(K).$$

这说明 $[a_1,b]\in H_3Z(K)$, 从而 $[a_1,b,b]\in H_4$. 由于 $[a_1,b,b]\neq 1$, $H_4\neq 1$, 从而 $c(H)\geqslant 4$. 这与定理 12.1.6 矛盾; 若 $d(H/Z(K))=3$, 由 p^4 阶群的分类可知存在 $d\in H$ 使得

$$H/Z(K)=K/Z(K)\times\langle dZ(K)\rangle \quad 或 \quad H/Z(K)=K/Z(K)*\langle dZ(K)\rangle.$$

取 $k\in K$, 由命题 1.1.9 计算可得 $[d^p,k]=[d,k]^p$. 因为 $\exp(G')=p$, 所以对于 $k\in K$ 有 $[d^p,k]=1$. 从而 $d^p\in Z(K)$, 只有

$$H/Z(K)=K/Z(K)\times\langle dZ(K)\rangle.$$

则 $d^p\in Z(K)$, $[K,d]\in Z(K)$. 由于 $a_2=[a_1,b]\notin\langle a_1,d\rangle$, 由定理 12.1.7 可知 $[a_1,d]=1$. 同理可知 $[b,d]=1$, 从而 $d\in Z(H)$. 此时 $\langle a_2d,b\rangle$ 既不交换也不正规, 矛盾.

情形 2 K 为上面所列的 (1) 型群.

这种情况与情形 1 是类似的. 事实上, 只要在 (2) 型群中让 $n=4$, 就会得到 (1) 中的 (i), (ii) 型群.

情形 3 K 为上面所列的 (3) 型群或 (4) 型群.

由定理 12.1.7, $H'\leqslant\langle c,a\rangle\bigcap\langle c,b\rangle=\langle c,a^p,b^p\rangle$. 从而

$$H'=K',\quad H_3=K_3=\langle a^p,b^p\rangle.$$

因为 H/K_3 为导群 p 阶的 p^4 阶群, 由 p^4 阶群的分类易知存在 $d\in H\backslash K$ 使得 $[a,d]\equiv[b,d]\equiv 1(\mathrm{mod}\ K_3)$. 由于 $\exp(H')=p$, 利用命题 1.1.9 计算可得

$$[a,d^p]=[a,d]^p=1,\quad [b,d^p]=[b,d]^p=1.$$

从而 $d^p\in Z(K)=K_3$. 因为 $c\notin\langle a,d\rangle$, 由定理 12.1.7 可知 $[a,d]=1$. 同理可知 $[ac,d]=1$. 此时子群 $\langle a,cd\rangle$ 既不交换也不正规, 矛盾. □

引理 12.1.11 设 G 是导群初等交换的亚 Hamilton p 群. 若 G 的 $\mathcal{A}_2$ 子群都是类 2 的, 则 G 的幂零类也是 2.

证明 设 G 为极小阶反例. 则 $c(G)=3$.

首先证明 G 不满足 2-Engel 条件. 若否, 则由定理 12.1.3 可知 G 是 3 群. 此时, 存在 $x,y,z\in G$, 使得 $[x,y,z]\neq 1$. 由于 G 为极小阶反例, 有

$$G=\langle x,y,z\rangle \quad 且 \quad [x,y,z]^3=[x^3,y,z]=1.$$

由 $[x,yz,yz]=1$ 可得, $[x,y,z]=[z,x,y]$. 同理可知

$$[x,y,z]=[y,z,x]=[z,x,y].$$

设

$$[x,y]=c,\quad [y,z]=a,\quad [z,x]=b,\quad [x,y,z]=[y,z,x]=[z,x,y]=d.$$

则 $G'=\langle a,b,c,d\rangle$. 因为 $[b,y]=d\neq 1$, 所以 $\langle b,y\rangle$ 不交换, 从而 $\langle b,y\rangle\trianglelefteq G$. 所以我们有 $c=[x,y]\in\langle b,y\rangle$. 注意到 $[c,b]=[c,y]=1$. 不妨设 $c=y^{3t}d^w$. 从而

$$d=[c,z]=[y^{3t}d^w,z]=[y^{3t},z]=1.$$

矛盾.

由于 G 不满足 2-Engel 条件, 存在 $[x,y,y]\neq 1$. 由 G 为极小阶反例可知

$$G=\langle x,y\rangle \quad 且 \quad [x,y,y]^p=1,\quad [x,y,x]^p=1.$$

令 $[x,y]=c$, $[c,y]=b$ 且 $[c,x]=a$. 则 $G_3=\langle b,a\rangle, G'=\langle c,G_3\rangle$. 若 $[c,x]\in\langle b\rangle$, 经过替换不妨设 $[c,x]=a=1$. 所以总有 $\langle a\rangle\bigcap\langle b\rangle=1$.

G 有 $p+1$ 个极大子群, 分别是 $M=\langle x^iy,\Phi(G)\rangle$ 和 $K=\langle x,\Phi(G)\rangle$, 其中 $i=0,1,\cdots,p$, $\Phi(G)=\langle x^p,y^p,c,a,b\rangle$. 易知 $\Phi(G)$ 是交换群.

因为 $[x,x^iy]=[x,y]=c$, $[c,x^iy]=a^ib\neq 1$, 所以 $N=\langle c,x^iy\rangle$ 是 x^iy 在 G 中的正规闭包, 并且 N 是内交换群. 由定理 12.1.7, $G'\leqslant N$. 由于 $[cx^p,x^iy]=ba^{i+i\mathrm{C}_p^2}\neq 1$, $\langle cx^p,x^iy\rangle$ 也是内交换群, 从而 $\langle cx^p,x^iy\rangle=N$, 这使得 $x^p\in N$. 由于 $(x^iy)^p\equiv x^{ip}y^p \pmod{G'}$, $x^{ip}y^p\in N$, 进而 $y^p\in N$. 这说明 $\Phi(G)\leqslant N$, 从而 $M=N$ 是内交换群.

若 $[c,x]=a\neq 1$, 令 $L=\langle c,x\rangle$. 此时 L 是 x 在 G 中的正规闭包, 并且 L 是内交换群. 由定理 12.1.7, $G'\leqslant L$. 由于 $[cy^p,x]\neq 1$, $\langle cy^p,x\rangle$ 也是内交换群, 从而 $\langle cy^p,x\rangle=L$, 这使得 $y^p\in L$. 这说明 $\Phi(G)\leqslant L$, 从而 $K=L$ 是内交换群.

若 $[c,x]=a=1$ 且 p 为奇素数, 则 $[x,y^p]=1$, 从而 $[\Phi(G),x]=1$. 此时 K 为交换群.

若 $[c,x]=a=1$ 且 $p=2$, 则 $[x,y^2]=b\neq 1$. 所以 $L=\langle x,y^2\rangle\trianglelefteq G$, 并且 L 为内交换群. 由定理 12.1.7, $G'\leqslant L$. 此时, $K=L$ 为内交换群.

由上可知, G 的极大子群都是内交换群或内交换群, 从而 G 是类 3 的 $\mathcal{A}_2$ 群, 这与 G 的 $\mathcal{A}_2$ 子群都类 2 相矛盾. □

定理 12.1.12 设 G 是导群初等交换的亚 Hamilton p 群且 $c(G)=3$. 则 G 是 $\mathcal{A}_2$ 群.

证明　若 G 不是 $\mathcal{A}_2$ 群, 则由引理 12.1.10 可知 G 的 $\mathcal{A}_2$ 子群都是类 2 的. 再由引理 12.1.11 可知 $c(G)=2$, 矛盾. □

最后, 再给出一个简单的推论.

推论 12.1.13　设 G 为导群初等交换的亚 Hamilton p 群且 $c(G)=3$. 则 $d(G)=2$ 且 p 为奇素数.

证明　由定理 12.1.12, G 为 $\mathcal{A}_2$ 群. 再由推论 12.1.9 可得最终的结论. □

12.2　导群初等交换的亚 Hamilton p 群的分类

本节分类导群初等交换的亚 Hamilton p 群.

定理 12.2.1　设 G 为有限亚 Hamilton p 群且 $\exp(G')=p$. 则 G 为以下互不同构的群之一.

(A) 导群 p 阶的群.

(B) 幂零类为 3 的群. 此时, $p\geqslant 3$, $d(G)=2$ 且 $G\in\mathcal{A}_2$.

(B1) $\langle a_1,b,a_2,a_3 \mid a_1^p=a_2^p=a_3^p=b^{p^m}=1,[a_1,b]=a_2,[a_2,b]=a_3,[a_3,b]=1,[a_i,a_j]=1\rangle$, 其中 $p\geqslant 3$, $1\leqslant i,j\leqslant 3$, 当 $m=1$ 时 $p\geqslant 5$.

(B2) $\langle a_1,b,a_2 \mid a_1^p=a_2^p=b^{p^{m+1}}=1,[a_1,b]=a_2,[a_2,b]=b^{p^m},[a_1,a_2]=1\rangle$, 其中 $p\geqslant 3$.

(B3) $\langle a_1,b,a_2 \mid a_1^{p^2}=a_2^p=b^{p^m}=1,[a_1,b]=a_2,[a_2,b]=a_1^{\nu p},[a_1,a_2]=1\rangle$, 其中 $p\geqslant 3$, $\nu=1$ 或者是一个固定的模 p 的平方非剩余.

(B4) $\langle a_1,a_2,b \mid a_1^9=a_2^3=1,b^3=a_1^3,[a_1,b]=a_2,[a_2,b]=a_1^{-3},[a_2,a_1]=1\rangle$.

(B5) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=c,[c,a]=b^{\nu p},[c,b]=a^p\rangle$, 其中 $p\geqslant 5$, ν 是一个固定的模 p 的平方非剩余.

(B6) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=c,[c,a]=a^{-p}b^{-lp},[c,b]=a^{-p}\rangle$, 其中 $p\geqslant 5$, $4l=\rho^{2r+1}-1$, $r=1,2,\cdots,\frac{1}{2}(p-1)$, ρ 是模 p 的最小原根.

(B7) $\langle a,b,c \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^3\rangle$.

(B8) $\langle a,b,c \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^{-3}\rangle$.

(C) $c(G)=2$ 且 $G'\cong \mathrm{C}_p^2$.

(C1) $K\times A$, 其中 $K=\langle a_1,a_2,b \mid a_1^4=a_2^4=1,b^2=a_1^2,[a_1,a_2]=1,[a_1,b]=a_2^2,[a_2,b]=a_1^2\rangle$, A 为满足 $\exp(A)\leqslant 2$ 的交换群.

(C2) $K\times A$, 其中 $K=\langle a_1,a_2,b,d \mid a_1^4=a_2^4=1,b^2=a_1^2,d^2=a_2^2,[a_1,a_2]=1,[a_1,b]=a_2^2,[a_2,b]=a_1^2,[a_1,d]=a_1^2,[a_2,d]=a_1^2a_2^2,[b,d]=1\rangle$, A 为满足 $\exp(A)\leqslant 2$ 的交换群.

(C3) $K\times A$, 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=$

$a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, $m_1 \geqslant m_2 \geqslant m_3$, 若 $p = 2$ 则 $m_1 > 1$, A 为满足 $\exp(A) \leqslant p^{m_2}$ 的交换群.

(C4) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{\nu p^{m_1}}\rangle$, $p > 2$, ν 为一个固定的模 p 的平方非剩余, $m_1 - 1 = m_2 \geqslant m_3$ 或者 $m_1 = m_2 \geqslant m_3$, A 为满足 $\exp(A) \leqslant p^{m_2}$ 的交换群.

(C5) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{kp^{m_1}} a_2^{-p^{m_2}}\rangle$, 若 $p > 2$, 则 $1 + 4k \notin (\mathrm{F}_p)^2$. 若 $p = 2$, 则 $k = 1$, $m_1 = m_2 \geqslant m_3$, A 为满足 $\exp(A) \leqslant p^{m_2}$ 的交换群.

(C6) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}}\rangle$, $m_1 - 1 = m_2 \geqslant m_3$, A 为满足 $\exp(A) \leqslant p^{m_2}$ 的交换群.

(C7) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, $m_1 \geqslant m_2 = m_3 + 1$, A 为满足 $\exp(A) \leqslant p^{m_3}$ 的交换群.

(C8) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = 1\rangle$, $p > 2$, ν 为一个固定的模 p 的平方非剩余, $m_1 \geqslant m_2 = m_3 + 1$ 或者 $m_1 > m_2 = m_3$, A 为满足 $\exp(A) \leqslant p^{m_3}$ 的交换群.

(C9) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{kp^{m_2}} a_3^{-p^{m_3}}, [a_2, a_3] = 1\rangle$, 若 $p > 2$, 则 $1 + 4k \notin (\mathrm{F}_p)^2$. 若 $p = 2$, 则 $k = 1$, $m_1 > m_2 = m_3$, A 为满足 $\exp(A) \leqslant p^{m_3}$ 的交换群.

(C10) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_1^{p^{m_1}}, [a_2, a_3] = 1\rangle$, $m_1 \geqslant m_2 = m_3 + 1$, A 为满足 $\exp(A) \leqslant p^{m_3}$ 的交换群.

(D) $c(G) = 2$ 且 $G' \cong \mathrm{C}_p^3$.

(D1) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_2, a_3] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{\eta p^{m_2}}, [a_1, a_2] = a_3^{p^{m_3}}, [a_3^p, a_1] = [a_3^p, a_2] = 1\rangle$, 其中 $p > 2$, $m_1 = m_2 + 1 = m_3 + 1$, η 为一个固定的模 p 的平方非剩余, A 为满足 $\exp(A) \leqslant p^{m_3}$ 的交换群.

(D2) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_2, a_3] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{lp^{m_2}} a_3^{-p^{m_2}}, [a_1, a_2] = a_3^{p^{m_3}}, [a_3^p, a_1] = [a_3^p, a_2] = 1\rangle$, 其中 $p > 2$, $m_1 = m_2 + 1 = m_3 + 1$, $1 + 4l \notin (\mathrm{F}_p)^2$, A 为满足 $\exp(A) \leqslant p^{m_3}$ 的交换群.

(D3) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{2^{m_1+1}} = a_2^{2^{m_2+1}} = a_3^{2^{m_3+1}} = 1, [a_2, a_3] = a_1^{2^{m_1}}, [a_3, a_1] = a_2^{2^{m_2}}, [a_1, a_2] = a_2^{2^{m_2}} a_3^{2^{m_3}}, [a_3^2, a_1] = [a_3^2, a_2] = 1\rangle$, 其中 $m_1 = m_2 + 1 = m_3 + 1$, A 为满足 $\exp(A) \leqslant 2^{m_3}$ 的交换群.

(D4) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_2, a_3] =$

$a_1^{p^{m_1}}, [a_1, a_3] = a_2^{\eta p^{m_2}}, [a_1, a_2] = a_3^{p^{m_3}}, [a_3^p, a_1] = [a_3^p, a_2] = 1\rangle$, 其中 $p > 2$, $m_1 = m_2 = m_3 + 1$, η 为一个固定的模 p 的平方非剩余, A 为满足 $\exp(A) \leqslant p^{m_3}$ 的交换群.

(D5) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_2, a_3] = a_1^{p^{m_1}}, [a_1, a_3] = a_1^{p^{m_1}} a_2^{lp^{m_2}}, [a_1, a_2] = a_3^{p^{m_3}}, [a_3^p, a_1] = [a_3^p, a_2] = 1\rangle$, 其中 $p > 2$, $m_1 = m_2 = m_3 + 1$, $1 + 4l \notin (\mathrm{F}_p)^2$, A 为满足 $\exp(A) \leqslant p^{m_3}$ 的交换群.

(D6) $K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{2^{m_1+1}} = a_2^{2^{m_2+1}} = a_3^{2^{m_3+1}} = 1, [a_2, a_3] = a_1^{2^{m_1}} a_2^{2^{m_2}}, [a_3, a_1] = a_2^{2^{m_2}}, [a_1, a_2] = a_3^{2^{m_3}}, [a_3^2, a_1] = [a_3^2, a_2] = 1\rangle$, 其中 $m_1 = m_2 = m_3 + 1$, A 为满足 $\exp(A) \leqslant 2^{m_3}$ 的交换群.

(D7) $K \times A$, 其中 $K = \langle a, b, c \mid a^4 = b^4 = c^4 = 1, [b, c] = a^2 b^2, [c, a] = b^2 c^2, [a, b] = c^2, [c^2, a] = [c^2, b] = 1\rangle$, A 为满足 $\exp(A) \leqslant 2$ 的交换群.

证明 由定理 12.1.6 可得 $c(G) \leqslant 3$. 若 $c(G) = 3$, 由定理 12.1.12 可得 $G \in \mathcal{A}_2$. 检查定理 9.3.1 的群表可得群 (B1)—(B8). 下面设 $c(G) = 2$. 取 N 为 G 的内交换子群. 由定理 12.1.7 可得 $G' \leqslant N$. 因为 $G' \leqslant Z(G)$, 所以 $G' \leqslant \Omega_1(Z(N)) = \Omega_1(\Phi(N))$. 从而由定理 1.7.10 可得 $G' \leqslant \mathrm{C}_p^3$. 若 $G' \cong \mathrm{C}_p$, 则 G 为定理中的 (A) 型群. 若 $G' \cong \mathrm{C}_p^2$, 由下面的引理 12.2.2 可知 G 为定理中的 (C1)—(C10) 型群. 若 $G' \cong \mathrm{C}_p^3$, 由引理 12.2.3 可得定理中的 (D1)—(D5) 型群. 验证可知, 这些群是互不同构亚 Hamilton p 群. 细节略去. □

引理 12.2.2 设 G 是亚 Hamilton p 群. 若 $G' \cong \mathrm{C}_p^2$ 且 $c(G) = 2$, 则 G 为定理 12.2.1 中的 (C1)—(C10) 型群之一.

证明 设 G/G' 的型不变量为 $(p^{m_1}, p^{m_2}, \cdots, p^{m_r})$, 其中 $m_1 \geqslant m_2 \geqslant \cdots \geqslant m_r$. 再设

$$G/G' = \langle a_1G' \rangle \times \langle a_2G' \rangle \times \cdots \times \langle a_rG' \rangle,$$

其中 $o(a_iG') = p^{m_i}$, $i = 1, 2, \cdots, r$. 则 $G = \langle a_1, a_2, \cdots, a_r \rangle$.

若 $m_1 = 1$, 则 G/G' 为初等交换 p 群. 任取 G 的两个非交换的元素 x, y, 由定理 12.1.7 可知, $G' \leqslant \langle x, y \rangle$, 从而 $\langle x, y \rangle$ 为 p^4 阶的内交换群. 这样的群为 $\mathcal{T}_4$ 群, 从而 G 为定理 10.6.9 中的群 (2) 和 (3), 或引理 10.6.10 中的群 (4)—(6). 此为定理中的 (C1), (C2) 型群以及 $m_1 = m_2 = m_3 = 1$ 时的 (C3)—(C5) 型群. 以下设 $m_1 > 1$.

设 i 是使 a_i 不在 $Z(G)$ 中的最小的正整数, 即存在 $j > i$ 使 $[a_i, a_j] \neq 1$. 若 $i \neq 1$, 说明 a_1 在 $Z(G)$ 中, 从而 $[a_1a_j, a_i] \neq 1$, 此时, 用 a_1a_j 替换 a_1, 仍然有其他的关系成立. 所以不妨设 $i = 1$, 即 $a_1 \notin Z(G)$.

再设 j 是使 $[a_1, a_j] \neq 1$ 成立的最小的正整数. 若 $j \neq 2$, 说明 $[a_1, a_2] = 1$, 从而 $[a_1, a_2a_j] \neq 1$, 此时, 用 a_2a_j 替换 a_2, 仍然有上面的关系成立. 所以不妨设 $j = 2$, 即 $[a_1, a_2] \neq 1$.

再设 k 是使 $[a_k, a_l] \notin \langle [a_1, a_2] \rangle$ 成立的最小正整数. 若 $k > 2$, 说明对所有的 s

都有

$$[a_1, a_s] \in \langle [a_1, a_2] \rangle, \quad [a_2, a_s] \in \langle [a_1, a_2] \rangle.$$

(1) 若 $[a_1, a_l] = 1$, 则

$$[a_1, a_2a_l] = [a_1, a_2], \quad [a_2a_l, a_k] = [a_2, a_k][a_l, a_k] \notin \langle [a_1, a_2] \rangle.$$

此时用 a_2a_l 替换 a_2, 仍然有其他的关系成立. 所以不妨设 $k \leqslant 2$.

(2) 若 $[a_1, a_l] = [a_1, a_2]^{\alpha}$, 其中 $(\alpha, p) = 1$, 再设 $[a_1, a_k] = [a_1, a_2]^{\beta}$, 则

$$[a_1, a_ka_l^{\alpha^{-1}\beta}] = 1, \quad [a_1, a_2a_ka_l^{\alpha^{-1}\beta}] = [a_1, a_2],$$

$$[a_2a_ka_l^{\alpha^{-1}\beta}, a_l] = [a_2, a_l][a_k, a_l] \notin \langle [a_1, a_2] \rangle.$$

此时用 $a_2a_ka_l^{\alpha^{-1}\beta}$ 替换 a_2, 仍然有其他的关系成立. 所以不妨设 $k \leqslant 2$.

再设 l 是使 $[a_k, a_l] \notin \langle [a_1, a_2] \rangle$ 的最小正整数. 若 $l \neq 3$, 则

$$[a_1, a_3] \in \langle [a_1, a_2] \rangle, \quad [a_2, a_3] \in \langle [a_1, a_2] \rangle.$$

从而

$$[a_k, a_3a_l] = [a_k, a_3][a_k, a_l] \notin \langle [a_1, a_2] \rangle.$$

此时用 a_3a_l 替换 a_3, 仍然有其他的关系成立. 所以不妨设 $l = 3$.

令 $K = \langle a_1, a_2, a_3 \rangle$, 则 $|K'| = |G'| = p^2$. 这样的 K 已经被定理 7.1.7 分类. 检查表 7.4 可知, K 为定理 12.2.1 中的 (C3)—(C10) 型群之一. 若 $r = 3$, K 已经是群 G. 下面设 $r \geqslant 4$ 并逐一进行讨论.

情形 1 K 为定理 12.2.1 中的 (C3)—(C6) 型群之一.

此时, $G' = \langle a_1^{p^{m_1}}, a_2^{p^{m_2}} \rangle$ 并且 $[a_1, a_3] = a_2^{p^{m_2}}$. 设 $a_4^{p^{m_4}} = a_1^{\alpha p^{m_1}} a_2^{\beta p^{m_2}}$. 用 $a_4a_1^{-\alpha p^{m_1 - m_4}}$ 替换 a_4 可得 $a_4^{p^{m_4}} = a_2^{\beta p^{m_2}}$.

若 $p > 2$ 或者 $m_2 > 1$, 用 $a_4a_2^{-\beta p^{m_2 - m_4}}$ 替换 a_4 后有 $a_4^{p^{m_4}} = 1$. 若 $p = 2$ 且 $m_2 = 1$. 断言存在 $x \in \{a_4, a_4a_2\}$ 使得 $x^2 \in \langle a_1^{2^{m_1}} \rangle$. 若否, 则 $a_4^2 = a_2^2$. 因为 $[a_4, a_2] = (a_4a_2)^2 \notin \langle a_1^{2^{m_1}} \rangle$, 所以 $\langle a_4, a_2 \rangle$ 非交换. 由定理 12.1.7 可知 $a_1^{2^{m_1}} \in \langle a_4, a_2 \rangle$. 进一步有 $[a_4, a_2] = a_1^{2^{m_1}} a_2^2$. 因而 $\langle a_4a_2, a_2a_1^{2^{m_1 - 1}} \rangle$ 既不交换也不正规, 矛盾. 用 x 或者 $xa_1^{2^{m_1 - 1}}$ 替换 a_4, 有 $a_4^2 = 1$.

因此, 总可设 $a_4^{p^{m_4}} = 1$. 断言 $[a_1, a_4] \in \langle a_2^{p^{m_2}} \rangle$. 若否, 可设 $[a_1, a_4] = a_1^{\gamma p^{m_1}} a_2^{\alpha p^{m_2}}$, 其中 $(\gamma, p) = 1$. 计算可得, $\langle a_1, a_4a_3^{-\alpha} \rangle$ 既不交换也不正规, 矛盾. 因此 $[a_1, a_4] \in \langle a_2^{p^{m_2}} \rangle$.

令 $L = \langle a_1, a_2, a_4 \rangle$. 若 $[a_1, a_4] \neq 1$, 则经过合适的替换不妨设 $[a_1, a_4] = a_2^{p^{m_2}}$. 此时, 断言 $L' = G'$. 若否, 则 $L' = \langle a_2^{p^{m_2}} \rangle$. 因为 $G' \nleqslant \langle a_2, a_4 \rangle$, 由定理 12.1.7 可

得 $[a_2,a_4]=1$. 因为 $K'=G'$, 所以 $K'=\langle a_2^{p^{m_2}},[a_2,a_3]\rangle$. 因此不妨设 $[a_2,a_3]=a_1^{sp^{m_1}}a_2^{tp^{m_2}}$, 其中 $(s,p)=1$. 若 $(t,p)=1$, 则 $\langle a_1^{sp^{m_1-m_2}}a_2^t,a_3a_4^{-1}\rangle$ 既不交换也不正规, 矛盾. 若 $t=0$ 且 $m_1>m_2$, 则 $\langle a_1a_2,a_3a_4^{-1}\rangle$ 既不交换也不正规, 矛盾. 若 $t=0$ 且 $m_1=m_2$, 则 $\langle a_1a_2,a_3a_4^{s-1}\rangle$ 既不交换也不正规, 也得到矛盾.

同理, 对于 $4\leqslant i\leqslant r$, 也不妨设 $a_i^{p^{m_i}}=1$ 以及 $[a_1,a_i]=1$ 或 $a_2^{p^{m_2}}$. 进一步有:

(*) 若 $[a_1,a_i]=a_2^{p^{m_2}}$, 则 $L'=G'$ 其中 $L=\langle a_1,a_2,a_i\rangle$.

对于 $3\leqslant i<j\leqslant r$, 由定理 12.1.7 可得 $[a_i,a_j]=1$.

令 j 为满足 $[a_1,a_j]=a_2^{p^{m_2}}$ 的最大正整数. 则 $[a_1,a_k]=1$ 对于 $j<k\leqslant r$ 成立. 对于 $3\leqslant k<j$, 若 $[a_1,a_k]=a_2^{p^{m_2}}$, 则 $[a_1,a_ka_j^{-1}]=1$. 如有必要用 $a_ka_j^{-1}$ 替换 a_k, 有 $[a_1,a_k]=1$.

令 $J=\langle a_1,a_2,a_j\rangle$. 因为 $J'=\langle a_1^{p^{m_1}},a_2^{p^{m_2}}\rangle$, 所以 J 为定理 12.2.1 中的 (C3)—(C6) 型群之一. 断言 $[a_2,a_k]=1$ 对于 $3\leqslant k\leqslant r$ 和 $k\neq j$ 成立. 若否, 分以下两种情形导出矛盾.

子情形 1.1 J 为定理 12.2.1 中的 (C3) 群之一.

此时, $[a_2,a_j]=1$. 可设 $[a_2,a_k]=a_2^{\gamma p^{m_2}}a_1^{\beta p^{m_1}}$ 其中 $(\beta,p)=1$. 若 $(\gamma,p)=1$, 则 $\langle a_1^{\beta p^{m_1-m_2}}a_2^{\gamma},a_k\rangle$ 既不交换也不正规, 矛盾. 若 $\alpha=0$ 且 $m_1>m_2$, 则 $\langle a_1a_2,a_k\rangle$ 既不交换也不正规, 矛盾. 若 $\alpha=0$ 且 $m_1=m_2$, 则 $\langle a_1a_2,a_ka_j^{\beta}\rangle$ 既不交换也不正规, 矛盾.

子情形 1.2 J 为定理 12.2.1 中的 (C4)—(C7) 型群之一.

此时, $[a_1,a_2]=1$ 且 $G'=\langle [a_2,a_j],a_2^{p^{m_2}}\rangle$. 因此可设 $[a_2,a_k]=a_2^{\gamma p^{m_2}}[a_2,a_j]^{\beta}$ 其中 $(\beta,p)=1$. 令 $x=a_k^{-\beta^{-1}}a_j$. 则 $[a_1,x]=a_2^{p^{m_2}}$ 且 $[a_2,x]=a_2^{-\beta^{-1}\gamma p^{m_2}}$. 若 $(\gamma,p)=1$, 则 $\langle a_2,a_ka_j^{-\beta}\rangle$ 既不交换也不正规, 矛盾. 若 $\alpha=0$, 则 $\langle a_1,a_2,x\rangle'=\langle a_2^{p^{m_2}}\rangle$. 这与 (*) 矛盾.

对于情形 1, 有 $G=J\times A$ 其中 $A=\langle a_3\rangle\times\cdots\times\langle a_{j-1}\rangle\times\langle a_{j+1}\rangle\times\cdots\times\langle a_r\rangle$. 因此得到定理 12.2.1 中的 (C3)—(C7) 型群之一.

情形 2 K 为定理 12.2.1 中的 (C7)—(C10) 型群之一.

此时, $G'=\langle a_s^{p^{m_s}},a_3^{p^{m_3}}\rangle$ 其中 $s=1$ 或 2, $[a_1,a_2]=a_3^{p^{m_3}}$ 且 $[a_2,a_3]=1$. 可设 $a_4^{p^{m_4}}=a_s^{\alpha p^{m_s}}a_3^{\beta p^{m_3}}$.

若 $p>2$ 或 $m_3>1$, 用 $a_4a_s^{-\alpha p^{m_s-m_4}}a_3^{-\beta p^{m_3-m_4}}$ 去替换 a_4 后可得 $a_4^{p^{m_4}}=1$. 若 $p=2$, $m_3=1$ 且 $m_s>1$, 断言存在 $x\in\{a_4,a_4a_3\}$ 使得 $x^2\in\langle a_s^{2^{m_s}}\rangle$. 若否, 则 $a_4^2=a_s^{\alpha 2^{m_s}}a_3^2$. 用 $a_4a_s^{-\alpha p^{m_s-m_4}}$ 去替换 a_4 后可得 $a_4^2=a_3^2$. 因为 $[a_4,a_3]=(a_4a_3)^2\notin\langle a_s^{2^{m_s}}\rangle$, 所以 $\langle a_4,a_3\rangle$ 非交换. 由定理 12.1.7 可得 $G'\leqslant\langle a_4,a_3\rangle$. 因此 $[a_4,a_3]=a_s^{2^{m_s}}a_3^2$. 计算可得, $\langle a_4a_3,a_3a_s^{2^{m_s-1}}\rangle$ 既不交换也不正规. 用 x 或 $xa_s^{2^{m_s-1}}$ 替换 a_4 后可得 $a_4^2=1$. 若 $p=2$ 且 $m_s=m_3=1$, 由 $m_1>1$ 可知 $s=2$. 因此 K 为 (C9) 型群. 此时, $[a_1,a_3]=a_2^2a_3^2$. 断言在 $\{a_4,a_4a_2,a_4a_3,a_4a_2a_3\}$ 中存在 2 阶元.

若否, 因为 $a_4^2\neq 1$, 所以有

$$a_4^2=a_2^2, a_3^2 \quad 或 \quad a_2^2a_3^2.$$

若 $a_4^2=a_3^2$, 分别用 a_3, a_2a_3 替换 a_2, a_3 后可得 $a_4^2=a_2^2$. 若 $a_4^2=a_2^2a_3^2$, 分别用 a_2a_3, a_2 替换 a_2, a_3 后可得 $a_4^2=a_2^2$. 因此不妨设 $a_4^2=a_2^2$. 因为 $(a_4a_2)^2=[a_4,a_2]\neq 1$, 所以 $L=\langle a_4,a_2\rangle$ 非交换. 由定理 12.1.7 可知 $G'\leqslant L$. 因此可设 $[a_4,a_2]=a_3^2a_2^{2\alpha}$. 若 $[a_4,a_2]=a_3^2a_2^2$, 则 $\langle a_1a_4,a_2\rangle$ 既不交换也不正规, 矛盾. 若 $[a_4,a_2]=a_3^2$, 则 $(a_4a_2)^2=a_3^2$. 因为 $(a_4a_2a_3)^2\neq 1$, 所以

$$[a_4a_2,a_3]=[a_4,a_3]=(a_4a_2a_3)^2\neq 1.$$

因为 $M=\langle a_4a_2,a_3\rangle$ 非交换, 由定理 12.1.7 可知 $G'\leqslant\langle a_4a_2,a_3\rangle$. 因此可设

$$[a_4,a_3]=[a_4a_2,a_3]=a_2^2a_3^{2\alpha}.$$

因为 $(a_4a_3)^2\neq 1$, 所以 $[a_4,a_3]\neq a_2^2a_3^2$. 因此 $[a_4,a_3]=a_2^2$. 此时, $\langle a_1a_4a_2,a_3\rangle$ 既不交换也不正规, 矛盾.

综上所述, 不妨设 $a_4^{p^{m_4}}=1$. 令 $\{s,t\}=\{1,2\}$. 因为 $G'\not\leqslant\langle a_t,a_4\rangle$, 由定理 12.1.7 可知 $[a_t,a_4]=1$. 由 (C7)—(C10) 型群的定义关系可知 $m_t>m_3$. 因为 $G'\not\leqslant\langle a_ta_3,a_4\rangle$, 由定理 12.1.7 可知 $[a_ta_3,a_4]=1$. 因此 $[a_3,a_4]=1$. 断言 $[a_s,a_4]\in\langle a_3^{p^{m_3}}\rangle$. 若否, 则可设 $[a_s,a_4]=a_s^{\alpha p^{m_s}}a_3^{\beta p^{m_3}}$, 其中 $(\alpha,p)=1$. 计算可得, $\langle a_s,a_t^{\beta}a_4^{s-t}\rangle$ 既不交换也不正规, 矛盾. 因此可设 $[a_s,a_4]=a_3^{\beta p^{m_3}}$.

进一步断言 $[a_s,a_4]=1$. 若否, 则 $(\beta,p)=1$ 且经过替换后可得 $[a_s,a_4]=a_3^{p^{m_3}}$. 下面分三种子情形推出矛盾.

子情形 2.1 $s=2,t=1$ 且 $m_2>m_3$.

此时, K 为 (C7), (C8) 型群之一. 由 (C7), (C8) 型群的定义关系可知, $[a_1,a_3]=a_2^{\eta p^{m_2}}$ 其中 $\eta=1$ 或者 ν. 计算可得, $\langle a_1a_4,a_2a_3\rangle$ 既不交换也不正规, 矛盾.

子情形 2.2 $s=2,t=1$ 且 $m_2=m_3$.

此时, K 为 (C8), (C9) 型群之一. 若 K 为 (C8) 型群, 则 $[a_1,a_3]=a_2^{\nu p^{m_2}}$. 计算可得, $\langle a_1a_4^{1-\nu},a_2a_3\rangle$ 既不交换也不正规, 矛盾. 若 K 为 (C9) 型群, 则 $[a_1,a_3]=a_2^{kp^{m_2}}a_3^{-p^{m_3}}$ 其中 $(k,p)=1$. 计算可得, $\langle a_1a_4,a_2^ka_3^{-1}\rangle$ 既不交换也不正规, 矛盾.

子情形 2.3 $s=1,\ t=2$.

此时, K 为 (C10) 型群. 由 (C10) 型群的定义关系, $[a_1,a_3]=a_1^{p^{m_3}}$. 计算可得, $\langle a_1,a_2a_3a_4^{-1}\rangle$ 既不交换也不正规, 依然得到矛盾.

综上所述, $[a_s,a_4]=1$. 同理可得, 对于 $4\leqslant i\leqslant r$, 都有 $a_i^{p^{m_i}}=1$. 进一步,

$$[a_1,a_i]=[a_2,a_i]=[a_3,a_i]=1.$$

对于 $4 \leqslant i < j \leqslant r$, 由定理 12.1.7 可得 $[a_i, a_j] = 1$. 此时, $G = K \times A$ 其中 $A = \langle a_4 \rangle \times \langle a_5 \rangle \times \cdots \times \langle a_r \rangle$. 因此得到定理 12.2.1 中的 (C7)—(C10) 型群. □

引理 12.2.3 设 G 为亚 Hamilton p 群. 若 $G' \cong \mathrm{C}_p^3$ 且 $c(G) = 2$, 则 G 为定理 12.2.1 中的 (D1)—(D7) 型群之一.

证明 设 G/G' 的型不变量为 $(p^{m_1}, p^{m_2}, \cdots, p^{m_r})$, 其中 $m_1 \geqslant m_2 \geqslant \cdots \geqslant m_r$. 再设

$$G/G' = \langle a_1G' \rangle \times \langle a_2G' \rangle \times \cdots \times \langle a_rG' \rangle,$$

其中 $o(a_iG') = p^{m_i}$, $i = 1, 2, \cdots, r$. 则 $G = \langle a_1, a_2, \cdots, a_r \rangle$. 若 $[a_i, a_j] \neq 1$, 则由定理 12.1.7 可得

$$G' = \langle a_i^{p^{m_i}}, a_j^{p^{m_j}}, [a_i, a_j] \rangle.$$

因此我们有

(*) 若 $a_i^{p^{m_i}} = 1$, 则 $a_i \in Z(G)$.

设 i 是使 $a_i^{p^{m_i}} \neq 1$ 的最小正整数. 若 $i \neq 1$, 则

$$a_1^{p^{m_1}} = \cdots = a_{i-1}^{p^{m_{i-1}}} = 1,$$

并且进一步由 (*) 有 $a_1, \cdots, a_{i-1} \in Z(G)$. 断言 $m_i = m_1$. 若否, 则 $(a_1a_j)^{p^{m_1}} = 1$ 对于 $j \geqslant i$ 成立. 由 (*) 可得 $a_1a_j \in Z(G)$. 从而对于 $j \geqslant i$ 有 $a_j \in Z(G)$ 成立. 这与 $|G'| = p^3$ 矛盾. 因此不妨设 $a_1^{p^{m_1}} \neq 1$.

再设 j 是使 $a_j^{p^{m_j}} \notin \langle a_1^{p^{m_1}} \rangle$ 得最小正整数. 若 $j \neq 2$, 则可设对于 $2 \leqslant k \leqslant j-1$ 有 $a_k^{p^{m_k}} = a_1^{\alpha_k p^{m_1}}$. 由定理 12.1.7 可知 $[a_k, a_1] = 1$. 用 $a_k a_1^{-\alpha_k p^{m_1 - m_k}}$ 去替换 a_k 后可得 $a_k^{p^{m_k}} = 1$. 由 (*) 可知, 对于 $2 \leqslant k \leqslant j-1$ 有 $a_k \in Z(G)$. 断言 $m_j = m_2$. 若否, 则对于 $k \geqslant j$ 有 $(a_2a_k)^{p^{m_2}} = 1$. 由 (*) 可知 $a_2a_k \in Z(G)$. 因此对于 $k \geqslant j$ 有 $a_2a_k \in Z(G)$. 这与 $|G'| = p^3$ 矛盾. 因此不妨设 $a_2^{p^{m_2}} \notin \langle a_1^{p^{m_1}} \rangle$.

再设 k 为使 $a_k^{p^{m_k}} \notin \langle a_1^{p^{m_1}}, a_2^{p^{m_2}} \rangle$ 的最小正整数. 若 $k \neq 3$, 则对于 $3 \leqslant w \leqslant k-1$ 可设 $a_w^{p^{m_w}} = a_1^{\alpha_w p^{m_1}} a_2^{\beta_w p^{m_2}}$. 断言 $m_k = m_3$. 若否, 则 $m_3 > m_k$. 不妨设 $m_{k-1} > m_k$. 用 $a_w a_1^{-\alpha_w p^{m_1 - m_w}} a_2^{\beta_w p^{m_2 - m_w}}$ 替换 a_w 后可得 $a_w^{p^{m_w}} = 1$. 由 (*) 可知, 对于 $3 \leqslant w \leqslant k-1$ 有 $a_w \in Z(G)$. 对于 $w \geqslant k$, 因为 $(a_3a_w)^{p^{m_3}} = 1$, 所以由 (*) 可得 $a_3a_w \in Z(G)$. 因而对于 $w \geqslant k$ 有 $a_w \in Z(G)$. 这与 $|G'| = p^3$ 矛盾. 因此可设 $a_3^{p^{m_3}} \notin \langle a_1^{p^{m_1}}, a_2^{p^{m_3}} \rangle$.

若 $r = 3$, 由定理 7.1.35 可得 G 为定理 12.2.1 中的 (D1)—(D7) 型群之一. 接下来我们设 $r \geqslant 4$.

断言, 存在合适的 a_1, a_2, a_3 满足以下条件:

(**) 对所有的 $x \in G'$, 存在 $b \in \langle a_1, a_2, a_3 \rangle$ 使得 $x = b^{p^{m_3}}$.

若 (**) 成立, 则对于 $i>3$, 存在 $b_i\in\langle a_1,a_2,a_3\rangle$ 使得 $a_i^{p^{m_i}}=b_i^{p^{m_3}}$. 由定理 12.1.7 可得 $[a_i,b_i]=1$. 用 $a_ib_i^{-p^{m_3-m_i}}$ 替换 a_i 后可得 $a_i^{p^{m_i}}=1$. 由 (*) 可知 $a_i\in Z(G)$. 因此 G 为定理 12.2.1 中的 (D1)—(D7) 型群之一.

接下来证明存在合适的 a_1,a_2,a_3 满足条件 (**). 若 $p>2$ 或者 $m_2>1$, 则 (**) 自然成立. 因此只需要处理 $p=2$ 且 $m_2=1$ 的情况.

情形 1 $m_1>1$.

若 $[a_2,a_3]\neq 1$, 则由定理 12.1.7 我们可设 $[a_2,a_3]=a_2^{2i}a_3^{2j}a_1^{2^{m_1}}$. 若 $[a_2,a_3]=a_2^2a_3^{2j}a_1^{2^{m_1}}$, 则 $\langle a_2a_1^{2^{m_1-1}},a_3\rangle$ 既不交换也不正规, 矛盾. 若 $[a_2,a_3]=a_2^3a_1^{2^{m_1}}=(a_3a_1^{2^{m_1-1}})^2$, 则 $\langle a_3a_1^{2^{m_1-1}},a_3\rangle$ 既不交换也不正规, 矛盾. 因此 $[a_2,a_3]=a_1^{2^{m_1}}$. 这种情形下, 容易检验 $G'=\mho_{\{1\}}(\langle a_1,a_2,a_3\rangle)$. 因此 (**) 成立.

情形 2 $m_1=1$.

用与定理 12.2.1 的开头一段类似的证明方法, 可以选择适当的 a_1,a_2,a_3 使得 $K=\langle a_1,a_2,a_3\rangle$ 的换位子群的阶至少为 4.

若集合 $\{1,a_1,a_2,a_3,a_1a_2,a_1a_3,a_2a_3,a_1a_2a_3\}$ 中存在两个元素平方相等, 则由定理 12.1.7 知它们一定是可交换的元素. 此时

$$\{a_1,a_2,a_3,a_1a_2,a_1a_3,a_2a_3,a_1a_2a_3\}$$

中存在 2 阶元. 由 (*), 这个 2 阶元在 K 的中心. 这与 $|K'|\geqslant 4$ 矛盾. 因此

$$G'=\mho_{\{1\}}(K)=\{1,a_1^2,a_2^2,a_3^2,(a_1a_2)^2,(a_1a_3)^2,(a_2a_3)^2,(a_1a_2a_3)^2\}.$$

此时 (**) 也成立. □

12.3 导群非初等交换的亚 Hamilton p 群的分类

本节分类导群非初等交换的亚 Hamilton p 群.

定理 12.3.1 *设 G 为有限亚 Hamilton p 群且 $\exp(G')>p$. 则 G 为以下互不同构的群之一.*

(E) *G 为亚循环群.*

(E1) $\langle a,b\mid a^{p^{r+s+u}}=1,\ b^{p^{r+s+t}}=a^{p^{r+s}},\ a^b=a^{1+p^r}\rangle$, *其中 $r\geqslant 1$, $u\leqslant r$ 和 $r+1\geqslant s+u\geqslant 2$, 并且若 $p=2$, 则 $r\geqslant 2$;*

(E2) $\langle a,b\mid a^{2^3}=b^{2^m}=1,a^b=a^{-1}\rangle$, *其中 $m\geqslant 1$;*

(E3) $\langle a,b\mid a^{2^3}=1,b^{2^m}=a^4,a^b=a^{-1}\rangle$, *其中 $m\geqslant 1$;*

(E4) $\langle a,b\mid a^{2^3}=b^{2^m}=1,a^b=a^3\rangle$, *其中 $m\geqslant 1$.*

(F) *G 非亚循环但 G' 循环且 $|G'|\geqslant p^2$.*

(F1) $G = K \times A$, 其中 $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s}} = 1, a^b = a^{1+p^r}\rangle$, $u \leqslant r$, $r+1 > s+u \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-(s+u)}$ 的非平凡的交换群;

(F2) $G = K \times A$, 其中 $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}}\rangle$, $t \geqslant 1$, $r \geqslant u \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{t+(r+1)-u}$ 的非平凡的交换群;

(F3) $G = K \times A$, 其中 $K = \langle a, b \mid a^{p^{r+s}} = 1, b^{p^{r+s+t}} = 1, a^b = a^{1+p^r}\rangle$, $t \geqslant 1$, $r+1 > s \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-s}$ 的非平凡交换群;

(F4) $G = K \times A$, 其中 $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r}\rangle$, $stu \neq 0, r+1 > s+u \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-(s+u)}$ 的非平凡交换群;

(F5) $G = (K \rtimes B) \times A$, 其中 $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}}\rangle$, $B = \langle b_1\rangle \times \langle b_2\rangle \times \cdots \times \langle b_f\rangle$ 满足 $o(b_i) = p^{r_i}$, $[a, b_i] = a^{p^{r+t_i}}$, $[b, b_i] = 1$, $\max\{t, u-2\} < t_1 < t_2 < \cdots < t_f < t+u$, $r+t > r_1+t_1 > r_2+t_2 > \cdots > r_f+t_f \geqslant t+u \geqslant t+2$, A 是满足 $\exp(A) \leqslant p^{t+(r+1)-u}$ 的交换群.

(G) G' 的型不变量为 (p^α, p) 其中 $\alpha \geqslant 2$.

(G1) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+m_2}} = a_2^{p^{m_2+1}} = a_3^p = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, 其中 $m_1 > m_2 \geqslant 1$, p 为奇素数;

(G2) $G = K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+k}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, $m_1 \geqslant m_2 \geqslant m_3$, $1 \leqslant k \leqslant \min\{m_1 - m_3, m_2 - m_3 + 1, m_2 - 1\}$, A 是满足 $\exp(A) \leqslant p^{m_2-k}$ 的交换群.

证明　若 G 亚循环, 则由引理 12.3.2 可得 G 为定理中的 (E1)—(E4) 型群之一. 下面设 G 非亚循环. 若 G' 循环, 则由引理 12.3.6 可得 G 为定理中的 (F1)—(F5) 型群之一. 若 G' 非循环, 则由引理 12.3.7 可知 G 为定理中的 (G1) 型和 (G2) 型群之一. 验证可知, 这些群是互不同构亚 Hamilton p 群. 细节略去. □

引理 12.3.2　设 G 为亚循环 p 群且 $|G'| \geqslant p^2$. 若 G 为亚 Hamilton 群, 则 G 为定理 12.3.1 中的 (E1)—(E4) 型群之一.

证明　分两种情形讨论.

情形 1　$p > 2$ 或者 G 为通常的亚循环 2 群, 即

$$G = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r}\rangle,$$

其中 $r \geqslant 1$, $u \leqslant r$, 并且若 $p = 2$ 则 $r \geqslant 2$.

因为 $|G'| \geqslant p^2$, 所以 $s+u \geqslant 2$. 我们只需证明 $r+1 \geqslant s+u$ 即可. 若否, 则 $r+1 < s+u$. 计算可得

$$[a^{p^{r+1}}, b] = a^{-p^{r+1}}(a^{p^{r+1}})^b = a^{p^{2r+1}} \neq 1.$$

因此 $\langle a^{p^{r+1}}, b\rangle$ 既不交换也不正规, 矛盾. 因而 $r+1 \geqslant s+u$, G 为定理 12.3.1 中的 (E1) 型群.

情形 2 $p=2$ 且 G 不是通常的亚循环 2 群.

令 $o(a)=2^n$ 且 $H=\langle a^{2^{n-2}},b\rangle$. 因为 $H'=\langle a^{2^{n-1}}\rangle$, 所以 H 非交换. 进而 $H\trianglelefteq G$. 由定理 12.1.7 可知 $a^2\in H$. 因此 $n\leqslant 3$ 且 $|G'|=4$. 由 [27] 中的命题 72.1 可知 $G\in\mathcal{A}_2$. 最后由 $\mathcal{A}_2$ 群的分类定理可得 G 为定理 12.3.1 中的 (E2)—(E4) 型群之一. □

定理 12.3.3 设 G 是二元生成的亚 Hamilton p 群且 $\exp(G')>p$. 则 G 亚循环.

证明 设 $G=\langle a,b\rangle$ 是极小阶的反例. 由定理 2.5.3 知, $\overline{G}:=G/\Phi(G')G_3$ 非亚循环. 因为 $|\overline{G}'|=p$, $\overline{G}$ 是内交换群. 由定理 1.7.10 知, $\overline{G}\cong \mathrm{M}_p(n,m,1)$. 因为 $\langle\bar{a}^p,\bar{b}\rangle$, $\langle\bar{b}^p,\bar{a}\rangle$, $\langle\overline{ab}^p,\bar{a}\rangle$, $\langle\overline{ab}^p,\bar{b}\rangle$ 均为 $\overline{G}$ 的不正规的子群, 所以它们在 G 中的完全反像也是 G 的不正规的子群, 从而是交换群. 所以

$$[a^p,b]=[b^p,a]=[(ab)^p,a]=[(ab)^p,b]=1. \tag{12.1}$$

下面分两种情况得出矛盾:

(i) $p=2$. 此时 $(ab)^2=a^2b^2[a,b]$. 由 (12.1) 式可知, $[a,b]\in Z(G)$, 从而 $G'=\langle[a,b]\rangle$. 再由 (12.1) 式, $[a,b]^2=[a^2,b]=1$. 这与 $\exp(G')>2$ 矛盾.

(ii) p 为奇素数. 由 (12.1) 式可得

$$[a,b,a]^p=[a^p,b,a]=1,\quad [a,b,b]^p=[a^p,b,b]=1,$$

即 $\exp(G_3)\leqslant p$. 再由 (12.1) 式, $[a,b]^p=[a^p,b]=1$. 这与 $\exp(G')>p$ 矛盾. □

下面的两个数论的引理将被用到, 在此列出, 证明从略.

引理 12.3.4 设 n 是正整数, $n\geqslant 2$. 令 $U=U(2^n)$ 是环 $\mathbb{Z}/2^n\mathbb{Z}$ 的可逆元组成的乘法群. 则

$$\begin{aligned}U&=\langle -1\rangle\times\langle 1+2^2\rangle(\cong \mathrm{C}_2\times \mathrm{C}_{2^{n-2}})\\&=\{\varepsilon+i2^m\mid \varepsilon=1\text{ 或 }-1,\ 2\leqslant m\leqslant n,\ 1\leqslant i<2^{n-m}\text{ 且 } i \text{ 是奇数}\}.\end{aligned}$$

又, 对 $m<n$, $\varepsilon+i2^m$ 的阶是 2^{n-m}, 且 $\langle\varepsilon+i2^m\rangle=\langle\varepsilon+j2^m\rangle$ 对任意奇数 j 成立.

引理 12.3.5 设 p 是奇素数, n 是正整数. 假定 $U=U(p^n)$ 是由 $\mathbb{Z}/p^n\mathbb{Z}$ 的可逆元组成的乘法群, 即

$$U=\{x\in\mathbb{Z}/p^n\mathbb{Z}\mid (x,p)=1\}.$$

设 $S(U)\in\mathrm{Syl}_p(U)$. 则

$$S(U)=\{x\in U\mid x\equiv 1(\mathrm{mod}\ p)\},$$

并且 $S(U)$ 是 p^{n-1} 阶循环的. $S(U)$ 的唯一的 p^i 阶子群 $S_i(U), 0 \leqslant i < n$ 是

$$S_i(U) = \{x \in U \mid x \equiv 1 (\mathrm{mod}\ p^{n-i})\}.$$

引理 12.3.6　设 G 为亚 Hamilton p 群且 G 非亚循环. 若 $|G'| \geqslant p^2$ 且 G' 循环, 则 G 为定理12.3.1中的 (F1)—(F5) 型群之一.

证明　由定理 12.3.3 可知, $d(G) > 2$. 设 $G' = \langle c \rangle$, G/G' 的型不变量为

$$(p^{m_1}, p^{m_2}, \cdots, p^{m_w}), \quad \text{其中} m_1 \geqslant m_2 \geqslant \cdots \geqslant m_w.$$

令

$$G/G' = \langle a_1G' \rangle \times \langle a_2G' \rangle \times \cdots \times \langle a_wG' \rangle, \quad \text{其中} o(a_iG') = p^{m_i}, i = 1, 2, \cdots, w.$$

则 $G = \langle a_1, a_2, \cdots, a_w \rangle$.

设 i 是使得 a_i 不在 $C_G(G/\mho_1(G'))$ 中的最小的正整数, 即存在 $j > i$ 使得 $G' = \langle [a_i, a_j] \rangle$. 若 $i \neq 1$, 说明 a_1 在 $C_G(G/\mho_1(G'))$ 中, 从而

$$[a_1a_j, a_i] \notin \mho_1(G'), \quad G' = \langle a_1a_j, a_i \rangle.$$

此时, 用 a_1a_j 来替换 a_1, 不妨设 $i = 1$, 即 $a_1 \notin C_G(G/\mho_1(G'))$.

再设 j 是使 $G' = \langle [a_1, a_j] \rangle$ 的最小的正整数. 若 $j \neq 2$, 说明 $[a_1, a_2] \in \mho_1(G')$. 此时, 用 a_2a_j 来替换 a_2, 不妨设 $j = 2$, 即 $G' = \langle [a_1, a_2] \rangle$.

设 $K = \langle a_1, a_2 \rangle$, 则由引理 12.3.3 可知, K 为亚循环群. 从而 K 为定理 12.3.2 中的群, 即 K 为定理 12.3.1 中的 (E1)—(E4) 型群之一. 下面分五步来证明定理.

第一步　K 是定理 12.3.1 中的 (E1) 型群.

若否, 则可设 $K = \langle a, b \rangle$ 满足定理 12.3.1 中 (E2)—(E4) 型群的定义关系, 即

$$a^{2^3} = 1, \quad b^{2^m} \in \mho_1(K_3) = \langle a^4 \rangle \quad \text{且} \quad [a, b] \equiv a^2 (\mathrm{mod}\ \mho_1(K_3)).$$

显然, $G' = K' = \langle a^2 \rangle$ 且 $m_3 = m_4 = \cdots = m_w = 1$.

情形 1　$a_3^2 \in \mho_1(K_3)$ 且 $[a_3, b] \in \mho_1(K_3)$.

此时, 若 $[a_3, b] = a^4$, 则子群 $\langle a_3, b \rangle$ 既不交换也不正规, 矛盾; 若 $[a_3, b] = 1$, 则 $[a_3a^2, b] = a^4$, 从而子群 $\langle a_3a^2, b \rangle$ 既不交换也不正规, 矛盾.

情形 2　$a_3^2 \in K_3$ 且 $[a_3, b] \equiv a^2 \ (\mathrm{mod}\ K_3)$.

若 $[a_3, a] \in K_3$, 则 $[a_3, a^2] = [a_3, a]^2 = 1$, 即 $[a_3, G'] = 1$. 计算可得, $1 = [a_3^2, b] = [a_3, b]^2[a_3, b, a_3] = [a_3, b]^2$, 从而 $[a_3, b] \in K_3$, 矛盾. 所以一定有 $[a_3, a] \equiv a^2 \ (\mathrm{mod}\ K_3)$. 此时, $(a_3a)^2 \in K_3$ 且 $[a_3a, b] \in K_3$. 用 a_3a 替换 a_3 可转化为情形 1 得出矛盾.

情形 3　$a_3^2 \equiv a^2 (\mathrm{mod}\ K_3)$.

若 $[a_3, a] \in K_3$, 则 $(a_3a)^2 \in K_3$. 此时, 用 a_3a 替换 a_3 可转化为情形 1 或情形 2 得出矛盾. 以下不妨设 $[a_3, a] \equiv a^2 (\mathrm{mod}\ K_3)$.

因为 $a_3^2\equiv a^2(\bmod K_3)$, 所以 $[a_3^2,b]=[a^2,b]=a^4$. 从而必有 $[a_3,b]\equiv a^2(\bmod K_3)$. 注意到此时 $(a_3a)^2\equiv a^2(\bmod K_3)$, 同理有 $[a_3a,b]\equiv a^2(\bmod K_3)$. 这使得 $[a,b]\in K_3$, 矛盾.

第二步 通过替换, 不妨设 $a_i^{p^{m_i}}=1$, 其中 $3\leqslant i\leqslant w$. 从而 $[a_i,a_j]=1$ 对于 $3\leqslant i,j\leqslant w$ 成立.

由第一步, $K\cong\langle r,s,t,u\rangle_p$ 且满足 $r\geqslant 1$, $u\leqslant r$ 和 $r+1\geqslant s+u$. 若 $p=2$, 则还有 $r\geqslant 2$. 设 $K=\langle a,b\mid a^{p^{r+s+u}}=1,b^{p^{r+s+t}}=a^{p^{r+s}},a^b=a^{1+p^r}\rangle$.

令 $L=\langle a,a_i\rangle$, 并且设 x_i 是使 $L=\langle a,x_i\rangle$ 成立且 $\langle x_i\rangle\bigcap\langle a\rangle$ 最小的元素, 我们断言 $x_i^{p^{m_i}}=1$. 若否, 设

$$\langle x_i\rangle\bigcap\langle a\rangle=\langle a^{p^\alpha}\rangle,\quad \langle[x_i,a]\rangle=\langle a^{p^\beta}\rangle,$$

其中 $\alpha\geqslant r$, $\beta\geqslant r$. 则存在与 p 互素的整数 y 和 z 使得 $x_i^{p^{m_i}}=a^{yp^\alpha}$, $[x_i,a]=a^{zp^\beta}$. 用命题 1.1.10 计算可得

$$\begin{aligned}(x_ia^{-yp^{\alpha-m_i}})^{p^{m_i}}&=x_i^{p^{m_i}}[x_i,a^{yp^{\alpha-m_i}}]^{\binom{p^{m_i}}{2}}[x_i,a^{yp^{\alpha-m_i}},x_i]^{\binom{p^{m_i}}{3}}a^{-yp^\alpha}\\&=a^{yzp^{\alpha+\beta-m_i}\binom{p^{m_i}}{2}}[a^{yzp^{\alpha+\beta-m_i}\binom{p^{m_i}}{3}},x_i].\end{aligned}$$

注意到当 $p=2$ 时, $\beta\geqslant r\geqslant 2$. 我们总有 $(x_ia^{-yp^{\alpha-m_i}})^{p^{m_i}}\in\langle a^{p^{\alpha+1}}\rangle$, 这与 x_i 的取法矛盾.

用上面的 x_i 去替换 a_i, 不妨设 $a_i^{p^{m_i}}=1$, 其中 $3\leqslant i\leqslant w$.

对于 $3\leqslant i,j\leqslant w$, 因为 $\langle a_i,a_j\rangle$ 不包含 G', 断言 $[a_i,a_j]=1$. 若否, 由定理 12.1.7 可得 $G'\leqslant\langle a_i,a_j\rangle$. 易知 $\langle a_i,a_j\rangle$ 非亚循环. 这与定理 12.3.3 矛盾.

第三步 将 K 按是否可裂, 分别写成如下四种群.

(A) $K=\langle a,b\mid a^{p^{r+s+u}}=1,b^{p^{r+s}}=1,a^b=a^{1+p^r}\rangle$, 其中, $r+1\geqslant s+u\geqslant 2$, 且若 $p=2$ 则 $r\geqslant 2$;

(B) $K=\langle a,b\mid a^{p^{r+t+u}}=1,b^{p^r}=1,a^b=a^{1+p^{r+t}}\rangle$, 其中 $t\geqslant 1$, $r\geqslant u\geqslant 2$;

(C) $K=\langle a,b\mid a^{p^{r+s}}=1,b^{p^{r+s+t}}=1,a^b=a^{1+p^r}\rangle$, 其中 $t\geqslant 1$, $r+1\geqslant s\geqslant 2$, 且若 $p=2$ 则 $r\geqslant 2$;

(D) $K=\langle a,b\mid a^{p^{r+s+u}}=1,b^{p^{r+s+t}}=a^{p^{r+s}},a^b=a^{1+p^r}\rangle$, 其中, $stu\neq 0$, $r+1\geqslant s+u\geqslant 2$, 且若 $p=2$ 则 $r\geqslant 2$.

K 仍如第二步所设. 当 $t=0$ 时, 计算可得, 对于奇素数 p 有 $(ba^{-1})^{p^{r+s}}=1$, 对于 $p=2$ 有 $(ba^{2^u-2^{r-1}-1})^{2^{r+s}}=1$. 用 ba^{-1} 或者 $ba^{2^u-2^{r-1}-1}$ 替换 b, 可得 (A) 型群.

以下设 $t\geqslant 1$. 当 $s=0$ 时, 计算可得 $(a^{-1}b^{p^t})^{p^r}=1$. 分别用 b 和 $a^{-1}b^{p^t}$ 替换 a 和 b, 可得 (B) 型群. 当 $u=0$ 以及 $su\neq 0$ 时, 易得 (C) 型群和 (D) 型群.

第四步　决定当 K 为直积因子时的群 G. 设 $G=K\times A$. 则易知 A 是非平凡的交换群.

情形 1　K 为第三步中的 (A) 型群.

任取 $d\in A$ 并设 $o(d)=p^e$. 计算可得, $[a^{p^{s+u-1}}d,b]=a^{p^{r+s+u-1}}\neq 1$. 从而

$$a^{p^r}\in\langle(a^{p^{s+u-1}}d)^{p^e}\rangle=\langle a^{p^{e+s+u-1}}\rangle.$$

这说明 $e+s+u-1\leqslant r$. 由 d 的任意性可得 $\exp(A)\leqslant p^{(r+1)-(s+u)}$. 因为 G 非亚循环, 所以 $A\neq 1$, 即 $r+1>s+u$. 因此 G 为定理 12.3.1 中的 (F1) 型群.

情形 2　K 为第三步中的 (B) 型群.

任取 $d\in A$, 并设 $o(d)=p^e$. 计算可得, $[a^{p^{u-1}}d,b]=a^{p^{r+t+u-1}}\neq 1$. 从而

$$a^{p^{r+t}}\in\langle(a^{p^{u-1}}d)^{p^e}\rangle=\langle a^{p^{e+u-1}}\rangle.$$

这说明 $e+u-1\leqslant r+t$. 由 d 的任意性可得 $\exp(A)\leqslant p^{t+(r+1)-u}$. 因此 G 为定理 12.3.1 中的 (F2) 型群.

情形 3　K 为第三步中的 (C) 型群或者 (D) 型群.

任取 $d\in A$ 并设 $o(d)=p^e$. 计算可得, $[a^{p^{s+u-1}}d,b]=a^{p^{r+s+u-1}}\neq 1$. 从而

$$a^{p^r}\in\langle(a^{p^{s+u-1}}d)^{p^e}\rangle=\langle a^{p^{e+s+u-1}}\rangle.$$

这说明 $e+s+u-1\leqslant r$. 由 d 的任意性可得 $\exp(A)\leqslant p^{(r+1)-(s+u)}$. 因为 G 非亚循环, 所以 $A\neq 1$. 即 $r+1>s+u$. 因此 G 为定理 12.3.1 中的 (F3) 型群或者 (F4) 型群.

第五步　决定当 K 不是直积因子时的群 G.

设 $G=H\times A$, 其中 K 在 H 中无直积因子. 则易知 $K<H$ 且 A 是交换群. 由第二步, 可设 $H=K\rtimes B$, 其中 $B=\langle b_1\rangle\times\langle b_2\rangle\times\cdots\times\langle b_f\rangle$ 满足 $o(b_i)=p^{r_i}$, $r\geqslant r_1\geqslant r_2\geqslant\cdots\geqslant r_f$.

首先说明 K 不能是第三步中的 (C) 型群和 (D) 型群. 若否, 通过计算可知 $\langle ab^{-p^t}\rangle\bigcap\langle a\rangle=1$. 因为子群 $\langle ab^{-p^t},b_i\rangle$ 不包含 G', 所以由定理 12.1.7 有 $[ab^{-p^t},b_i]=1$. 同理有 $[b,b_i]=1$, 从而 $H=K\times B$, 这与 H 的取法矛盾.

如果 K 是第三步中的 (A) 型群, 则一定有 $s=0$. 若否, 通过计算可知 $\langle ab\rangle\bigcap\langle a\rangle\leqslant\langle a^{p^{r+1}}\rangle$. 因为子群 $\langle ab,b_i\rangle$ 不包含 G', 所以由定理 12.1.7 有 $[ab,b_i]=1$. 同理有 $[b,b_i]=1$, 从而 $H=K\times B$, 这与 H 的取法矛盾.

综上所述, 我们可设

$$K=\langle a,b\mid a^{p^{r+t+u}}=1,b^{p^r}=1,a^b=a^{1+p^{r+t}}\rangle,$$

其中 $t \geqslant 0$ 且 $r \geqslant u \geqslant 2$. 因为 $G' \not\leqslant \langle b, b_i\rangle$, 所以由定理 12.1.7 可得 $[b, b_i] = 1$.

设 j 是使得 $[a, b_i]$ 的阶最大的最小的正整数. 不妨设 $j = 1$ (若 $j \neq 1$, 用 b_1b_j 替换 b_1). 同理, 不妨设

$$\langle [a, b_1]\rangle \geqslant \langle [a, b_2]\rangle \geqslant \cdots \geqslant \langle [a, b_f]\rangle.$$

设 $[a, b_i] = a^{\gamma_i p^{r+t_i}}$, 其中 $(\gamma_i, p) = 1$. 则 $t \leqslant t_1 \leqslant t_2 \leqslant \cdots \leqslant t_f$.

注意到 $a^b = a^{1+\gamma_i p^{r+t_i}}$. 由引理 12.3.4 和引理 12.3.5 知, 存在正整数 w 使得

$$(1 + \gamma_i p^{r+t_i})^j \equiv 1 + p^{r+t_i} \pmod{p^{r+t+u}}.$$

用 b_i^w 代替 b_i, 不妨设 $[a, b_i] = a^{p^{r+t_i}}$.

情形 1 $t_1 > t$.

若 $t_2 = t_1$, 则 $b_1b_2^{-1}$ 为 H 的直积因子, 矛盾. 所以 $t_1 < t_2$. 同理可得

$$t < t_1 < t_2 < \cdots < t_f.$$

若 $(b_1b^{-p^{t_1-t}})^{p^{r_1}} = 1$, 则 $b_1b^{-p^{t_1-t}}$ 为 H 的直积因子, 矛盾. 因此 $(b_1b^{-p^{t_1-t}})^{p^{r_1}} \neq 1$. 进一步有 $b^{p^{r_1+t_1-t}} \neq 1$. 从而 $r_1 + t_1 - t < r$. 因此

$$r - r_1 > t_1 - t > 0.$$

同理可得

$$r_i + t_i > r_{i+1} + t_{i+1}.$$

由引理 12.3.4 和引理 12.3.5 可得, 在由 $\mathbb{Z}/p^{r+t+u}\mathbb{Z}$ 的可逆元组成的乘法群中, $1 + p^{r+t_f}$ 的阶是 p^{t+u-t_f}. 由 $[a, b_f^{p^{r_f}}] = 1$ 可知,

$$a^{b_f^{p^{r_f}}} = a^{(1+p^{r+t_f})^{p^{r_f}}} = a.$$

所以还有 $r_f \geqslant t + u - t_f$, 即 $t_f + r_f \geqslant t + u$. 计算可得

$$\langle ba^{p^{t-t_1+u-1}}\rangle \bigcap \langle a\rangle = \langle (ba^{p^{t-t_1+u-1}})^{p^r}\rangle = \langle a^{p^{r+t-t_1+u-1}}\rangle.$$

令 $N = \langle ba^{p^{t-t_1+u-1}}, b_1\rangle$. 因为 $[ba^{p^{t-t_1+u-1}}, b_1] = a^{p^{r+t+u-1}} \neq 1$, 所以 N 非交换. 由定理 12.1.7 可知 $G' \leqslant N$. 所以 $r + t - t_1 + u - 1 \leqslant r + t$. 因而 $t_1 \geqslant u - 1$. 最后, 与第四步相同的方法可以得到 $\exp(A) \leqslant p^{t+(r+1)-u}$. 因此 G 为定理 12.3.1 中的 (F5) 型群. 这种情形下还有 $\exp(A) \leqslant p^r$.

情形 2 $t_1 = t$.

设 h 是使 $t_h = t$ 的最大的正整数. 令 $r' = r_h$, $t' = t + (r - r_h)$ 且 $\widetilde{K} = \langle a, b_h \rangle$. 则

$$\widetilde{K} = \langle a, b_h \mid a^{p^{r'+t'+u}} = 1, b_h^{p^{r'}} = 1, a^{b_h} = a^{1+p^{r'+t'}} \rangle.$$

若 $h < f$, 则设 $f' = f - h$. 对于 $1 \leqslant i \leqslant f'$, 令 $b'_i = b_{h+i}$, $t'_i = t_{h+i}$ 且

$$\widetilde{B} = \langle b'_1 \rangle \times \cdots \times \langle b'_{f'} \rangle, \quad \widetilde{H} = \widetilde{K} \rtimes \widetilde{B}, \quad \widetilde{A} = A \times \langle bb_h^{-1} \rangle \times \langle b_1 b_h^{-1} \rangle \times \cdots \times \langle b_{h-1} b_h^{-1} \rangle.$$

则 $G = \widetilde{H} \times \widetilde{A}$, 其中 $\widetilde{A}$ 尽可能大. 注意到 $t'_1 > t'$. 与情形 1 同理可得 G 为定理 12.3.1 中的 (F5) 型群.

若 $h = f$, 则仍有 $G = \widetilde{H} \times \widetilde{A}$. 与 $h < f$ 的情形不同之处是 $\widetilde{H} = \widetilde{K}$. 与第四步类似的讨论可得 $\exp(A) \leqslant p^{t'+(r'+1)-u}$. 因此 G 为定理 12.3.1 中的 (F2) 型群. □

引理 12.3.7　*设 G 为亚 Hamilton p 群. 若 $\exp(G') > p$ 且 G' 非循环, 则 G 为定理 12.3.1 中的 (G1), (G2) 型群之一.*

证明　设 H 为 G 的二元生成的子群, 满足 $\exp(H') > p$. 由定理 12.3.3 可知 H 为亚循环的. 又由定理 12.1.7 可知 $G' < H$, 从而 G' 也是亚循环的.

令 $N = \mho_1(G')$, $\overline{G} = G/N$, 则 $\overline{G}'$ 为 p^2 阶的初等交换群. 由定理 12.3.3 可知 $d(G) > 2$, 从而 $d(\overline{G}) > 2$. 再由推论 12.1.13 可知, $c(\overline{G}) = 2$. 从而 $\overline{G}$ 只能是引理 12.2.2 中的群, 即 $\overline{G}$ 为定理 12.2.1 中的 (C1)—(C10) 型群之一.

设 $\overline{G}$ 为定理 12.2.1 中的 (C1) 型群, 即 $\overline{G} = \overline{K} \times \overline{A}$, 其中

$$\overline{K} = \langle \bar{a}_1, \bar{a}_2, \bar{b} \mid \bar{a}_1^4 = \bar{a}_2^4 = 1, \bar{b}^2 = \bar{a}_1^2, [\bar{a}_1, \bar{a}_2] = 1, [\bar{a}_1, \bar{b}] = \bar{a}_2^2, [\bar{a}_2, \bar{b}] = \bar{a}_1^2 \rangle,$$

$\overline{A}$ 为满足 $\exp(\overline{A}) \leqslant 2$ 的交换群. 则

$$G' = \langle [a_1, b], [a_2, b], \mho_1(G') \rangle = \langle a_1^2, a_2^2 \rangle \quad 且 \quad \mho_1(G') = \langle a_1^4, a_2^4 \rangle.$$

设 M 为 $\mho_1(G')$ 的满足 $M \trianglelefteq G$ 的极大子群. 则可设

$$M = \langle e, \mho_2(G') \rangle, \quad [a_1, a_2] \equiv e^i (\bmod\ M),$$

$$b^2 \equiv a_1^2 e^j (\bmod\ M) \quad 且 \quad [a_1, b] \equiv a_2^2 e^k (\bmod\ M).$$

因为 $[a_1, a_2] \equiv e^i (\bmod\ M)$, 所以

$$[a_1^2, a_2] \equiv [a_1, a_2^2] \equiv 1\ (\bmod\ M).$$

因为 $b^2 \equiv a_1^2 e^j (\bmod\ M)$, 所以

$$[a_1^2, b] \equiv [a_1, b^2] \equiv 1\ (\bmod\ M).$$

另一方面, 因为 $[a_1,b]\equiv a_2^2e^k(\mathrm{mod}\ M)$, 所以

$$[a_1^2,b]\equiv[a_1,b]^2[a_1,b,a_1]\equiv a_2^4(\mathrm{mod}\ M).$$

从而 $a_2^4\in M$ 并且因此 $M=\langle a_1^8,a_2^4\rangle$.

令 $L=\langle a_1M,bM\rangle$. 因为 $\exp(L')=2$, 所以由定理 12.1.12 可得 $c(L)=2$. 因而 $[a_2^2,b]\equiv 1(\mathrm{mod}\ M)$. 另一方面,

$$[a_2^2,b]\equiv[a_2,b]^2[a_2,b,a_2]\equiv a_1^4(\mathrm{mod}\ M).$$

从而 $a_1^4\in M$. 因此 $M=\mho_1(G)$, 矛盾.

类似的推理可证 $\overline{G}$ 不是定理 12.2.1 中的 (C2) 型群.

设 $\overline{G}$ 为定理 12.2.1 中的 (C4) 型群. 即 $\overline{G}=\overline{K}\times\overline{A}$, 其中 $\overline{A}$ 为满足 $\exp(\overline{A})\leqslant p^{m_2}$ 的交换群, $\overline{K}=\langle\bar{a}_1,\bar{a}_2,\bar{a}_3\rangle$ 具有如下定义关系

$$\bar{a}_1^{p^{m_1+1}}=\bar{a}_2^{p^{m_2+1}}=\bar{a}_3^{p^{m_3}}=1,\quad[\bar{a}_1,\bar{a}_2]=1,\quad[\bar{a}_1,\bar{a}_3]=\bar{a}_2^{p^{m_2}},\quad[\bar{a}_2,\bar{a}_3]=\bar{a}_1^{\nu p^{m_1}},$$

其中 $p>2$, ν 是一个固定的模 p 的平方非剩余, $m_1-1=m_2\geqslant m_3$ 或 $m_1=m_2\geqslant m_3$. 则

$$G'=\langle[a_1,a_3],[a_2,a_3],\mho_1(G')\rangle=\langle[a_1,a_3],[a_2,a_3]\rangle=\langle a_1^{p^{m_1}},a_2^{p^{m_2}}\rangle.$$

因为 $\langle\bar{a}_1,\bar{a}_3\rangle$ 和 $\langle\bar{a}_2,\bar{a}_3\rangle$ 非亚循环, 所以 $\langle a_1,a_2\rangle$ 和 $\langle a_1,a_3\rangle$ 也非亚循环. 由定理 12.3.3 可得 $[a_1,a_2]^p=1$ 和 $[a_1,a_3]^p=1$. 进一步可得 $\exp(G')=p$, 矛盾.

类似的推理可以证明 $\overline{G}$ 不是定理 12.2.1 中的 (C5)—(C10) 型群.

最后, $\overline{G}$ 只能与定理 12.2.1 中的 (C3) 型群同构. 设 $\overline{G}=\overline{K}\times\overline{A}$. 其中 $\overline{A}$ 是满足 $\exp(\overline{A})\leqslant p^{m_2}$ 的交换群; $\overline{K}=\langle\bar{a}_1,\bar{a}_2,\bar{a}_3\rangle$ 具有定义关系

$$\bar{a}_1^{p^{m_1+1}}=\bar{a}_2^{p^{m_2+1}}=\bar{a}_3^{p^{m_3}}=1,\quad[\bar{a}_1,\bar{a}_2]=\bar{a}_1^{p^{m_1}},\quad[\bar{a}_1,\bar{a}_3]=\bar{a}_2^{p^{m_2}},\quad[\bar{a}_2,\bar{a}_3]=1,$$

其中 $m_1\geqslant m_2\geqslant m_3$. 若 $p=2$, 则 $m_1>1$. 此时 $G'=\langle a_1^{p^{m_1}},a_2^{p^{m_2}}\rangle$.

由于 $\langle\bar{a}_2,\bar{a}_3\rangle$ 不包含 G', 所以 $\langle a_2,a_3\rangle$ 也不包含 G'. 这说明 $[a_2,a_3]=1$. 同理, $\langle a_2,a_3a_1^{p^{m_1}}\rangle$ 也不包含 G', 从而 $[a_2,a_3a_1^{p^{m_1}}]=1$, 进而有 $[a_1^{p^{m_1}},a_2]=a_1^{p^{2m_1}}=1$. 设 a_1 的阶为 p^{m_1+1+k}, 其中 $k\geqslant 1$, 则有 $m_1>k$.

设 $\overline{A}=\langle\bar{a}_4\rangle\times\langle\bar{a}_5\rangle\times\cdots\times\langle\bar{a}_f\rangle$, 其型不变量为 $(p^{m_4},p^{m_5},\cdots,p^{m_f})$. 对于 $4\leqslant i\leqslant f$ 和 $1\leqslant j\leqslant f$, 由于 $\langle\bar{a}_i,\bar{a}_j\rangle$ 不包含 G', 所以 $\langle a_i,a_j\rangle$ 也不包含 G'. 这说明 $[a_i,a_j]=1$, 从而 $a_i\in Z(G)$. 设 $a_i^{p^{m_i}}=a_1^{sp^{m_1+1}}$, 则 $(a_ia_1^{-sp^{m_1+1-m_i}})^{p^{m_i}}=1$. 令

$$b_i=a_ia_1^{-sp^{m_1+1-m_i}},\quad A=\langle b_4\rangle\times\langle b_5\rangle\times\cdots\times\langle b_f\rangle.$$

并设 $K=\langle a_1,a_2,a_3\rangle$. 则 $G=K\times A$.

设 $[a_1,a_2]=a_1^{p^{m_1}}a_1^{up^{m_1+1}}$, 即 $a_1^{a_2}=a_1^{1+(1+up)p^{m_1}}$. 由引理 12.3.4 和引理 12.3.5 可知, 存在正整数 w 使得

$$(1+(1+up)p^{m_1})^j=1+p^{m_1}.$$

分别用 a_2^w 和 a_3^w 代替 a_2 和 a_3, 不妨设 $[a_1,a_2]=a^{p^{m_1}}$.

由于 $\langle\bar{a}_1,\bar{a}_3\rangle$ 非亚循环, 所以 $\langle a_1,a_3\rangle$ 也非亚循环. 由定理 12.3.3 可知 $[a_1,a_3]^p=1$. 设 $[a_1,a_3]=a_2^{p^{m_2}}d$, 其中 $d\in\mho_1(G')$, 则 $a_2^{p^{m_2+1}}d^p=1$. 这说明 $a_2^{p^{m_2+1}}\in\mho_2(G')$, 从而

$$N=\mho_1(G')=\langle a_1^{p^{m_1+1}},a_2^{p^{m_2+1}}\rangle=\langle a_1^{p^{m_1+1}}\rangle,\quad a_2^{p^{m_2+1}}\in\langle a_1^{p^{m_1+2}}\rangle.$$

由引理 12.3.4 和引理 12.3.5 可知, 在由 $\mathbb{Z}/p^{m_1+1+k}\mathbb{Z}$ 的可逆元组成的乘法群中, $1+p^{m_1}$ 的阶是 p^{k+1}. 由于 $a_1^{(1+p^{m_1})^{p^{m_2+1}}}=a_1^{a_2^{p^{m_2+1}}}=a_1$, 所以有 $k+1\leqslant m_2+1$, 即 $k\leqslant m_2$. 以下分两种情形讨论.

情形 1　$k=m_2$. 此时, $[a_1,a_2^{p^{m_2}}]\neq 1$ 并且有 $m_1>m_2$.

这时, 由于 $\langle a_1,a_3\rangle$ 的幂零类大于 2. 由推论 12.1.13 可知, p 为奇素数且 $\langle a_1,a_3\rangle$ 为 $\mathcal{A}_2$ 群. 若 $m_3>1$, 则有子群 $\langle a_1,a_2^{p^{m_2}}a_3^p\rangle$ 既不交换也不正规. 所以一定有 $m_3=1$. 若 $A\neq 1$, 则对任意的 $1\neq e\in A$, 有 $\langle a_1,a_2^{p^{m_2}}e\rangle$ 既不交换也不正规. 所以一定有 $A=1$. 设 $a_3^p=a_1^{vp^{m_1+1}}$, 则 $(a_3a_1^{-vp^{m_1}})^p=1$. 用 $a_3a_1^{-vp^{m_1}}$ 替换 a_3, 不妨设 $a_3^p=1$.

设 $[a_1,a_3]=a_2^{p^{m_2}}a_1^{wp^{m_1+1}}$, 即 $a_2^{p^{m_2+1}}a_1^{wp^{m_1+2}}=1$. 注意到 G 是 p^{m_2+1} 交换的. 我们有 $(a_2a_1^{wp^{m_1-m_2+1}})^{p^{m_2+1}}=1$. 再设

$$(a_2a_1^{wp^{m_1-m_2+1}})^{p^{m_2}}=a_2^{p^{m_2+1}}a_1^{wp^{m_1+2}}a_1^{xp^{m_1+m_2}}.$$

则

$$(a_2a_1^{wp^{m_1-m_2+1}}a_1^{-xp^{m_1}})^{p^{m_2}}=a_2^{p^{m_2}}a_1^{wp^{m_1+1}}=[a_1,a_3].$$

用 $a_2a_1^{wp^{m_1-m_2+1}}a_1^{-xp^{m_1}}$ 替换 a_2, 不妨设 $a_2^{p^{m_2+1}}=1$ 且 $[a_1,a_3]=a_2^{p^{m_2}}$. 在这种情形下, 得到了定理 12.3.1 中的 (G1) 型群.

情形 2　$k<m_2$. 此时 $[a_1,a_2^{p^{m_2}}]=1$.

由于 $[a_1,a_3,a_1]=1$, 故 $[a_1^p,a_3]=[a_1,a_3]^p=1$. 从而 $\langle a_1^p,a_2\rangle$ 与 a_3 交换. 这时 $\langle a_1,a_3\rangle$ 内交换. 由于 $\langle a_2,a_3a_1^{p^{m_1-m_3+1}}\rangle$ 不包含 G', 有 $[a_2,a_3a_1^{p^{m_1-m_3+1}}]=1$. 进而有

$$1=[a_1^{p^{m_1-m_3+1}},a_2]=a_1^{p^{2m_1-m_3+1}}.$$

从而 $2m_1-m_3+1\geqslant m_1+1+k$, 即 $m_1-m_3\geqslant k$. 由于 $\langle a_1,a_2^{p^{m_2-m_3+2}}a_3^p\rangle$ 不包含 G', 故 $[a_1,a_2^{p^{m_2-m_3+2}}a_3^p]=1$. 进而有

$$a_1^{a_2^{p^{m_2-m_3+2}}}=a_1^{(1+p^{m_1})^{p^{m_2-m_3+2}}}=a_1.$$

在由 $\mathbb{Z}/p^{m_1+1+k}\mathbb{Z}$ 的可逆元组成的乘法群中, 由于 $1+p^{m_1}$ 的阶是 p^{k+1}, 故 $m_2-m_3+2\geqslant k+1$, 即 $k\leqslant m_2-m_3+1$.

对任意的 $b\in A$, 设 $o(b)=p^e$. 由于 $\langle a_1, a_2^{p^{m_2-e+1}}b\rangle$ 不包含 G', 因此 $[a_1, a_2^{p^{m_2-e+1}}b]=1$. 进而有

$$a_1^{a_2^{p^{m_2-e+1}}}=a_1^{(1+p^{m_1})^{p^{m_2-e+1}}}=a_1.$$

由于在由 $\mathbb{Z}/p^{m_1+1+k}\mathbb{Z}$ 的可逆元组成的乘法群中, $1+p^{m_1}$ 的阶是 p^{k+1}, 所以有 $m_2-e+1\geqslant k+1$, 即 $e\leqslant m_2-k$. 由 b 的任意性有 $\exp(A)\leqslant p^{m_2-k}$.

设 $a_3^p=a_1^{vp^{m_1+1}}$, 则 $(a_3a_1^{-vp^{m_1}})^p=1$. 用 $a_3a_1^{-vp^{m_1}}$ 替换 a_3, 不妨设 $a_3^p=1$.

设 $[a_1,a_3]=a_2^{p^{m_2}}a_1^{wp^{m_1+1}}$, 即 $a_2^{p^{m_2+1}}a_1^{wp^{m_1+2}}=1$. 注意到 $c(G)=2$. 于是有

$$(a_2a_1^{wp^{m_1-m_2+1}})^{p^{m_2}}=a_2^{p^{m_2}}a_1^{wp^{m_1+1}}.$$

用 $a_2a_1^{wp^{m_1-m_2+1}}$ 替换 a_2, 不妨设 $a_2^{p^{m_2+1}}=1$ 且 $[a_1,a_3]=a_2^{p^{m_2}}$. 在这种情形下, 得到了定理 12.3.1 中的 (G2) 型群. □

第 13 章 临界 p 群

我们知道, 反证法是数学中最常用、最基本的论证方法. 例如, 设 G 是有限群. 欲证某个命题成立. 若使用反证法, 则可设 G 是使得该命题不成立的最小阶反例. 由此导出矛盾即可. 注意到, 由最小阶反例出发, 我们可引出所谓临界群的概念.

以 $\mathcal{P}$ 表示任一群性质, 比如循环、交换、亚交换等. 称群 G 为 $\mathcal{P}$ 群, 如果 G 具有性质 $\mathcal{P}$. 回顾一下, 设 $\mathcal{P}$ 为一群性质. 若群 G 不是 $\mathcal{P}$ 群, 但 G 的每个真子群皆为 $\mathcal{P}$ 群, 则称 G 为一个**内 $\mathcal{P}$ 群**; 若群 G 不是 $\mathcal{P}$ 群, 但 G 的每个真商群皆为 $\mathcal{P}$ 群, 则称 G 为一个**外 $\mathcal{P}$ 群**; 若群 G 不是 $\mathcal{P}$ 群, 但 G 的每个真截段皆为 $\mathcal{P}$ 群, 则称 G 为**一个极小非 $\mathcal{P}$ 群**.

上面这几种群, 习惯上人们称其为 $\mathcal{P}$ 临界群, 或临界群. 当 G 为有限 p 群时, 也称之为临界 p 群. 在研究群性质 $\mathcal{P}$ 时, 特别是为建立 $\mathcal{P}$ 群的充分条件, 这几种 $\mathcal{P}$ 临界群的概念将起着重要的作用.

应该注意的是, 国外多数群论文献中使用的术语和我们这里的不太一样. 他们一般只用 “极小非 $\mathcal{P}$ 群” 的术语, 多数情形下指的是 “内 $\mathcal{P}$ 群”. 请读者在阅读文献时加以注意.

我们熟知的经典的临界 p 群的例子是: 内交换 p 群、内亚循环 p 群、极小非正则 p 群等. Janko 在文献 [97] 中研究了内 Q_8 自由的 2 群, 即有限 2 群 G 的真子群均不含四元数群 Q_8, 但 G 含有子群 Q_8.

本章介绍另外三类临界群的分类, 即极小非 3 交换 3 群、极小非 $\mathcal{P}_2$-p 群以及内 $\mathcal{P}_2$-p 群的分类.

众所周知, p 交换 p 群是有限 p 群中 “接近” 交换群的一个重要群类. 例如, 当 $p=2$ 时, 2 交换群即为交换群. 不太寻常的是, 虽然 p 交换 p 群一定是正则的, 但极小非正则 p 群是特殊的一类极小非 p 交换 p 群. Mann 在文献 [149],[150],[152] 给出了极小非正则 p 群的深刻的必要条件, 利用其深入研究了正则 p 群. 然而给出极小非正则 p 群的分类是困难的. 由此可知, 给出极小非 p 交换 p 群的分类是不现实的. 然而对于 $p=3$, 曲海鹏等在文献 [188] 给出了极小非 3 交换 3 群的完全分类.

另一方面, 我们知道, 幂零类是 p 群的重要算术不变量. 它的大小对 p 群的结构有着深刻影响. 例如, 幂零类为 1 的群恰是交换群. 因而幂零类为 2 的 p 群也可看作是 “接近” 交换群的 p 群. A. Mann 在文献 [153] 猜想: 大多数 p 群是类 2 的.

并对这个猜想的合理性进行了详细的论述. 这一猜想既反映了类 2 群是有限 p 群中比较大的群类, 也反映了类 2 群在 p 群研究中的重要性. 宋蕾薇等在文献 [206] 中分类了极小非类 2 的 p 群. 而李璞金在他的博士论文 [124] 中研究了内 $\mathcal{P}_2$-p 群的 p 群, 并对于 $p>3$, 分类了内 $\mathcal{P}_2$-p 群的 p 群, 参见文献 [125]—[127]. 显然, 内 $\mathcal{P}_2$-p 群的 p 群的分类可看作是内交换 p 群分类的一个自然的、较大的推广.

13.1 极小非 3 交换 3 群的分类

p 交换 p 群是 p 群中的重要群类. 为了研究 p 交换性, Hobby 在文献 [86] 中提出了 p 换位子及 p 换位子群等概念. 在此基础上, 徐明曜进一步研究了这个问题, 他在文献 [240] 中提出了 p 中心、p 导群等一系列概念. 曲海鹏等在文献 [188] 继续研究 p 群的 p 交换性. 给出了极小非 p 交换 p 群的某些性质, 特别是给出了极小非 3 交换 3 群的完全分类. 本节介绍他们的结果.

设 G 为 p 群. 对任意的 $a,b\in G$, 定义 a,b 的 p **换位子**为 $b^{-p}a^{-p}(ab)^p$. 记作 $[a,b]_p$. 设 A,B 为 G 的两个正规子群. 定义 A,B 的 p **换位子群**为

$$\langle [a,b]_p,[b,a]_p \mid a\in A,b\in B\rangle.$$

记作 $[A,B]_p$. $\delta(G)=[G,G]_p$ 称为群 G 的 p **导群**.

$$\zeta(G)=\{g\in G \mid [g,x]_p=[x,g]_p=1,\ \forall x\in G\}$$

称为群 G 的 p **中心**. G 称为 p **交换的**, 若对任意的 $a,b\in G$, 恒有 $(ab)^p=a^pb^p$. G 称为**极小非 p 交换的**, 若 G 本身非 p 交换但其所有真子群及真商群皆 p 交换.

定理 13.1.1 设 G 为极小非 p 交换群, 且 $\exp(G)=p^e$. 则 G 有以下性质.

(1) $d(G)=2$;

(2) 对任意的 $1\leqslant s\leqslant e$ 和 $a,b\in G$, 有 $[a^{p^s},b]=[a,b^{p^s}]=[a,b]^{p^s}$;

(3) 对任意的 $1\leqslant s\leqslant e$, 有 $\Omega_s(G)=\Omega_{\{s\}}(G),\mho_s(G)=\mho_{\{s\}}(G)$ 且 $|G/\Omega_s(G)|=|\mho_s(G)|$;

(4) $\zeta(G)=\Phi(G)$;

(5) $\delta(G)$ 为 G 的唯一的极小正规子群, 于是 $Z(G)$ 循环;

(6) $\mho_2(G')=1$, 进而有 $\mho_2(G)\leqslant Z(G)$;

(7) G 是 p^2 交换的.

证明 (1) 若 $d(G)>2$, 则由 p 交换定义及 G 的极小性知 G 本身 p 交换, 与题设矛盾.

(2) 对任意的 $a,b\in G$, 都有 $\langle a,b^{-1}ab\rangle=\langle a,[a,b]\rangle<G$, 由 G 的极小性可得 $\langle a,b^{-1}ab\rangle$ 是 p 交换的. 从而对任意的 $1\leqslant s\leqslant e$, 都有

$$[a^{p^s}, b] = a^{-p^s}b^{-1}a^{p^s}b = a^{-p^s}(b^{-1}ab)^{p^s} = (a^{-1}b^{-1}ab)^{p^s} = [a, b]^{p^s}.$$

同理可证 $[a, b^{p^s}] = [a, b]^{p^s}$. 从而 $[a^{p^s}, b] = [a, b^{p^s}] = [a, b]^{p^s}$.

(3) 若 G 正则, 由定理 1.11.5 直接可得结论成立. 若 G 非正则, 则 G 为极小非正则群, 由文献 [149] 中的定理 2 或文献 [247] 中的定理 5.2.15 也可知该结论成立.

(4) 首先证 $\zeta(G) \leqslant \Phi(G)$. 若存在 $1 \neq x \in \zeta(G)$ 且 $x \notin \Phi(G)$, 则由 (1) 可知存在 $y \in G$ 使得 $G = \langle x, y\rangle$. 而由 [243] 中的引理 1 知, G 是 p 交换的, 与题设矛盾, 从而 $\zeta(G) \leqslant \Phi(G)$. 下证 $\Phi(G) \leqslant \zeta(G)$. 对任意的 $a \in \Phi(G), b \in G$, 有 $\langle a, b\rangle < G$, 因而 a, b 是 p 交换的. 又由 b 的任意性可得 $a \in \zeta(G)$, 从而 $\Phi(G) \leqslant \zeta(G)$. 故有 $\zeta(G) = \Phi(G)$.

(5) 设 N 为 G 的极小正规子群, 由 G 的极小性得 G/N 是 p 交换的. 从而 $\delta(G) \leqslant N$. 又因为 G 非 p 交换, 所以 $\delta(G) \neq 1$, 且由 N 是 G 的极小正规子群可得 $|N| = p$, 故可得 $\delta(G) = N$. 又由 N 的任意性可得 G 的极小正规子群唯一, 从而 $Z(G)$ 的 p 阶子群唯一, $Z(G)$ 为循环群.

(6) 设 $G = \langle a, b\rangle$. 则 $G' = \langle [a, b]^g \mid g \in G\rangle$. 下证 $[a, b]^{p^2} = 1$. 设 $H = \langle a^p, b\rangle$, $H < G$. 由 G 的极小性得 H 是 p 交换的, 又由 [244] 中的Ⅵ, 定理 2.2 可知 $\mho_1(H) \leqslant Z(H)$, 从而 $[b^p, a^p] = 1$. 由 (2) 知 $[b^p, a^p] = [b, a]^{p^2}$, 即有 $[a, b]^{p^2} = 1$. 又因为 G' 是 p 交换的, 从而 $\mho_2(G') = 1$. 又对任意的 $x, y \in G$, 由 (2) 有 $[x^{p^2}, y] = [x, y]^{p^2}$, 从而有 $[x^{p^2}, y] = 1$, $x^{p^2} \in Z(G)$. 由 x 的任意性可得 $\mho_2(G) \leqslant Z(G)$.

(7) 由 (5) 可得 $|\delta(G)| = p$, 故对任意的 $x, y \in G$, 都有 ${[x, y]_p}^p = 1$. 由 p 换位子的定义有

$${[x, y]_p}^p = (y^{-p}x^{-p}(xy)^p)^p.$$

又 $\mho_1(G) < G$, 从而 $\mho_1(G)$ 是 p 交换的, 即得

$$1 = {[x, y]_p}^p = (y^{-p}x^{-p}(xy)^p)^p = y^{-p^2}x^{-p^2}(xy)^{p^2}.$$

故有 $(xy)^{p^2} = x^{p^2}y^{p^2}$. 由 x, y 的任意性即得 G 是 p^2 交换的. □

定理 13.1.2　设 G 为群. 则 G 为极小非 p 交换群当且仅当下列条件成立.

(1) $d(G) = 2$;

(2) $\zeta(G) = \Phi(G)$;

(3) $\delta(G)$ 为 G 的唯一的极小正规子群.

证明　$\Longrightarrow$: 由定理 13.1.1 即得.

$\Longleftarrow$: 由 $\delta(G) \neq 1$ 可得 G 非 p 交换, 故只需证 G 的所有真子群和真商群都是 p 交换群即可. 设 $M \lessdot G$. 因为 $\zeta(G) = \Phi(G)$, 所以 $\zeta(G) < M$. 又由 $d(G) = 2$ 可得 $|M : \zeta(G)| = |M : \Phi(G)| = p$. 故可设 $M = \langle x, \zeta(G)\rangle$, 其中 $x \in G \setminus \zeta(G)$. 由 [243] 中的引理 1 可得 M 是 p 交换的, 又由 M 的任意性得 G 的所有真子群都是 p 交换

群. 由 $\delta(G)$ 为 G 的唯一的极小正规子群可知, $\delta(G)$ 包含于 G 的任一非平凡的正规子群中. 故欲证 G 的所有真商群 p 交换, 只需证 $G/\delta(G)$ 是 p 交换群即可. 而这是显然的, 结论得证. □

定理 13.1.3 设 G 为有限亚交换的极小非 p 交换群, 则 $c(G) \leqslant p$.

证明 只需证明 $G_{p+1} = 1$ 即可. 对任意的 $a_1, a_2, \cdots, a_{p+1} \in G$, 令 $d_2 = [a_1, a_2]$. 由 $\langle d_2, a_3 \rangle < G$ 知 $\langle d_2, a_3 \rangle$ 是 p 交换的, 由 [244] 中的Ⅳ, 定理 3.6 得 $c(\langle d_2, a_3 \rangle) < p$, 从而 $[d_2, (p-1)a_3] = 1$. 又由 [244] 中的Ⅳ, 定理 3.4 得, 对任意的 $a_3, a_4 \in G$, 有 $[d_2, (p-2)a_4, a_3]^{(p-1)!} = 1$. 因为 $((p-1)!, p) = 1$, 所以 $[d_2, a_3, (p-2)a_4] = 1$. 令 $d_3 = [d_2, a_3]$. 再由 [244] 中的Ⅳ, 定理 3.4 可知, 对任意的 $a_4, a_5 \in G$, $[d_3, a_4, (p-3)a_5]^{(p-2)!} = 1$. 因为 $((p-2)!, p) = 1$, 又得 $[d_3, a_4, (p-3)a_5] = 1$. 反复应用 [244] 中的Ⅳ, 定理 3.4 $p-1$ 次, 即可得到对任意的 $a_1, a_2, \cdots, a_{p+1} \in G$ 都有 $[a_1, a_2, \cdots, a_{p+1}] = 1$ 成立. 故 $G_{p+1} = 1$. 从而 $c(G) \leqslant p$. □

下面分类极小非 3 交换 3 群. 首先证明几个引理.

引理 13.1.4 设 G 为极小非正则 3 群, 则 $c(G) = 3$.

证明 设 G 为极小非正则 3 群, 由 [247] 中的定理 5.2.15 可知 $d(G) = 2$, 从而有 $d(G/\mho_1(G)) = 2$. 又 $\exp(G/\mho_1(G)) = 3$, 由 [89] 中的Ⅲ, 定理 6.6 知 $|G/\mho_1(G)| \leqslant 3^3$. 因此 $c(G/\mho_1(G)) \leqslant 2$. 又由 [247] 中的定理 5.2.15 知 $\mho_1(G) = Z(G)$, 故 $c(G) \leqslant 3$. 若 $c(G) < 3$, 则 G 正则, 与题设矛盾. 故必有 $c(G) = 3$. □

引理 13.1.5 极小非 3 交换 3 群是亚交换群.

证明 若 G 正则, 则 G 为二元生成的正则 3 群, 由 [244] 中的Ⅳ, 定理 3.12 知 G' 循环, 从而 G 是亚交换群. 故可设 G 非正则, 则 G 为极小非正则 3 群, 由引理 13.1.4 有 $c(G) = 3$, 即 $G_4 = 1$. 又 $G'' \leqslant G_4$, $G'' = 1$, 故 G 亚交换. 结论得证. □

引理 13.1.6 设 G 为正则的极小非 3 交换 3 群, 则 G' 为 3^2 阶循环群.

证明 由定理 13.1.1(1) 有 $d(G) = 2$, 即 G 为二元生成的正则 3 群, 由 [244] 中的Ⅳ, 定理 3.12 有 G' 循环. 又由定理 13.1.1(6) 有 $\mho_2(G') = 1$. 设 $G' = \langle c \rangle$, 则有 $o(c) \leqslant 3^2$. 由 G 非 3 交换可得 $G' \neq 1$. 若 $o(c) = 3$, 即 G' 为 3 阶循环群, 从而 G 为 3 交换群, 与题设矛盾. 故必有 $o(c) = 3^2$. □

引理 13.1.7 设 G 为极小非 3 交换 3 群且 G 非亚循环, 则 $\omega(G) = 3$.

证明 由 [244] 中的Ⅳ, 定理 5.3 可得 $\omega(G) \geqslant 3$, 即 $|G/\mho_1(G)| \geqslant 3^3$. 又

$$d(G/\mho_1(G)) = 2 \quad \text{且} \quad \exp(G/\mho_1(G)) = 3,$$

由 [89] 中的Ⅲ, 定理 6.6 得 $|G/\mho_1(G)| \leqslant 3^3$, 从而 $|G/\mho_1(G)| = 3^3$. 因此 $\omega(G) = 3$. □

引理 13.1.8 设 G 为极小非正则 3 群且 $\exp(G) = 3^e$. 则 $|G| = 3^{e+2}$.

证明 由引理 13.1.4 的证明过程可知, $|G/\mho_1(G)| \leqslant 3^3$. 又由 [247] 中的定理 5.2.15 知, $\mho_1(G)$ 为 3^{e-1} 阶循环群. 从而可得 $|G| \leqslant 3^{e+2}$. 由于 G 中存在 3^e 阶元,

若 $|G| \leqslant 3^{e+1}$, 则 G 为亚循环群. 故 G 正则, 与题设矛盾. 故 $|G| = 3^{e+2}$. □

定理 13.1.9 设 G 为有限正则 3 群且 $\exp(G) = 3^e$. 则 G 为极小非 3 交换 3 群当且仅当 G 是下列互不同构群之一.

(1) $G = \langle a, b \mid a^{3^{t+4}} = b^9 = 1, [a, b] = a^{3^{t+2}} \rangle$, t 为非负整数;

(2) $G = \langle a, b, c \mid a^{3^3} = 1, b^{3^{t+2}} = a^{3^2}, b^{-1}ab = a^4 \rangle$, t 为非负整数;

(3) $G = \langle a, b, c \mid a^9 = b^9 = c^9 = 1, [a, b] = c, [c, a] = [c, b] = 1 \rangle$;

(4) $G = \langle a, b, c \mid a^9 = b^9 = c^9 = 1, [a, b] = c, [c, a] = c^3, [c, b] = 1 \rangle$;

(5) $G = \langle a, b, c \mid a^{3^3} = b^{3^2} = 1, c^3 = a^{3^2}, [a, b] = c, [c, a] = [c, b] = 1 \rangle$;

(6) $G = \langle a, b, c \mid a^{3^3} = b^{3^2} = 1, c^3 = a^{3^2}, [a, b] = c, [c, a] = c^3, [c, b] = 1 \rangle$;

(7) $G = \langle a, b, c \mid a^{3^n} = b^{3^2} = 1, c^3 = a^{3^{n-1}}, [a, b] = c, [c, a] = 1, [c, b] = c^3 \rangle$, n 为 $\geqslant 4$ 的整数;

(8) $G = \langle a, b, c \mid a^{3^n} = b^{3^2} = 1, c^3 = a^{-3^{n-1}}, [a, b] = c, [c, a] = 1, [c, b] = c^3 \rangle$, n 为 $\geqslant 3$ 的整数.

其中群 (1)—(2) 是亚循环的, 群 (3)—(8) 是非亚循环的.

证明 设 G 为满足题设条件的群, 则由引理 13.1.5 知 G 为亚交换群, 由引理 13.1.3 得 $c(G) \leqslant 3$. 又由引理 13.1.6 可得 G' 为 3^2 阶循环群, 故可设 $G' = \langle c \rangle$ 且 $o(c) = 3^2$. 下面分 G 为亚循环群和非亚循环群两种情况讨论.

情形 1 G 为亚循环群.

由定理 6.1.3 可得

$$G = \langle a, b \mid a^{3^{r+s+u}} = 1, b^{3^{r+s+t}} = a^{3^{r+s}}, b^{-1}ab = a^{1+3^r} \rangle,$$

其中 s, t, u, r 为非负整数, 且 $r \geqslant 1, u \leqslant r$.

此时 $G' = \langle a^{3^r} \rangle = \langle c \rangle$, 故有 $o(a^{3^r}) = 3^{s+u} = 3^2$, 由此得 $s + u = 2$. 由定理 13.1.1(6) 有 $\mho_2(G) \leqslant Z(G)$, 从而 $\langle a^{3^2} \rangle \langle b^{3^2} \rangle \leqslant Z(G)$. 又由定理 13.1.1(5) 知 $Z(G)$ 循环, 故有 $\langle a^{3^2} \rangle \leqslant \langle b^{3^2} \rangle$ 或 $\langle b^{3^2} \rangle \leqslant \langle a^{3^2} \rangle$. 若 $\langle a^{3^2} \rangle \leqslant \langle b^{3^2} \rangle$, 则 $a^{3^2} \in \langle a \rangle \bigcap \langle b \rangle = \langle a^{3^{r+s}} \rangle$. 故 $3^{r+s} \leqslant 3^2$, 即 $r + s \leqslant 2$. 若 $\langle b^{3^2} \rangle \leqslant \langle a^{3^2} \rangle$, 则 $b^{3^2} \in \langle a \rangle \bigcap \langle b \rangle = \langle b^{3^{r+s+t}} \rangle$. 故 $3^{r+s+t} \leqslant 3^2$, 即 $r + s + t \leqslant 2$. 由此可得 $r + s \leqslant 2$. 现在有: r, s, u, t 满足关系式

$$s + u = 2, \quad r + s \leqslant 2, \quad r \geqslant 1, \quad u \leqslant r.$$

从而可得 (r, s, u, t) 只有两种取值: $(2, 0, 2, t)$ 与 $(1, 1, 1, t)$, 其中 t 为非负整数.

$(2, 0, 2, t)$ 对应的群为

$$\langle a_1, b_1 \mid a_1^{3^4} = 1, b_1^{3^{2+t}} = a_1^{3^2}, b_1^{-1}a_1b_1 = a_1^{1+3^2} \rangle. \tag{1'}$$

对群 $(1)'$, 令 $a = b_1, b = a^{-1}b^{3^t}$, 就得到了群 (1).

$(1,1,1,t)$ 对应的群为 $\langle a, b \mid a^{3^3}=1, b^{3^{2+t}}=a^{3^2}, b^{-1}ab=a^{1+3}\rangle$. 此为群 (2).

情形 2　G 为非亚循环群.

由引理 13.1.7 知 $w(G)=3$. 作 G 的 (L)-群列:

$$G > L > \Phi(G) > \mho_1(G).$$

取 $a \in G\backslash L$, $b \in L\backslash\Phi(G)$, $d \in \Phi(G)\backslash\mho_1(G)$ 满足 a,b,d 分别为 $G\backslash L$, $L\backslash\Phi(G)$, $\Phi(G)\backslash\mho_1(G)$ 中的任一最小阶元素. 由 [244] 中的Ⅳ, 定理 4.14 知 (a,b,d) 是 G 的一组唯一性基底, 设 G 的型不变量为 (n,m,r), 则 $o(a)=3^n, o(b)=3^m, o(d)=3^r$.

设 $G=\langle a,b\rangle$, $c=[a,b]$. 由定理 13.1.1 知

$$c^{3^n}=[a,b]^{3^n}=[a^{3^n},b]=1.$$

而 $o(c)=3^2$, 因而 $n\geqslant 2$, 同理可证 $m\geqslant 2$. 下证 $m=2$: 因为 G 是极小非 3 交换群, 由定理 13.1.1 知 G 是 3^2 交换的, 因此 $\mho_2(G)=\langle a^9,b^9\rangle$. 由 $\mho_2(G)\leqslant Z(G)$ 可得 $\mho_2(G)=\langle a^9\rangle\langle b^9\rangle$, 又由 a,b 的取法知 $\langle a\rangle\bigcap\langle b\rangle=1$, 故有 $\mho_2(G)=\langle a^9\rangle\times\langle b^9\rangle$. 因为 $Z(G)$ 循环, 故 $m\leqslant n$, 从而必有 $b^9=1$, 即 $m\leqslant 2$. 从而 $m=2$.

由以上讨论得: $n\geqslant 2$, $m=2$. 又由 G 非亚循环, 故 $c\notin\langle a\rangle$ 且 $c\notin\langle b\rangle$.

下面再分 $n=2$ 与 $n>2$ 两种情况讨论.

子情形 2.1　$n=2$.

断言 $\langle a\rangle\bigcap\langle c\rangle=1$ 且 $\langle b\rangle\bigcap\langle c\rangle=1$ 成立: 若 $c^3\in\langle a\rangle$, 则有 $c^3=a^{\pm 3}$. 又由 $\mho_1(G')\leqslant Z(G)$ 可知 $c^3\in Z(G)$, 从而

$$1=[c^3,b]=[a^{\pm 3},b]=[a^{\pm 1},b]^3.$$

而 $[a^{\pm 1},b]^3\neq 1$, 矛盾, 故 $c^3\notin\langle a\rangle$. 从而 $\langle a\rangle\bigcap\langle c\rangle=1$. 同理可证得 $\langle b\rangle\bigcap\langle c\rangle=1$.

下证 G 的型不变量为 $(2,2,2)$: 令 $H=\langle b\rangle\langle c\rangle$. 则 $H\trianglelefteq G$, $|G|=|\langle a\rangle||H|/|\langle a\rangle\bigcap H|$. 若 $|\langle a\rangle\bigcap H|\neq 1$, 则 $a^3\in H=\langle b\rangle\langle c\rangle$. 又由 $c^3\in Z(G)$ 可得 $\Omega_1(H)=\langle b^3\rangle\times\langle c^3\rangle$. 故 $a^3\in\langle b^3\rangle\times\langle c^3\rangle$. 因为 $\langle a\rangle\bigcap\langle c\rangle=1$, 且由 a,b 的取法知 $\langle a\rangle\bigcap\langle b\rangle=1$. 因此 $a^3=b^{\pm 3}c^{\pm 3}$. 令 $a_1=ac^{\mp 1}$. 由 [244] 中的Ⅳ, 定理 4.14 知 a_1,b,d 还是 G 的一组唯一性基底. 而由 $\langle a,c\rangle<G$ 知 $\langle a,c\rangle$ 是 p 交换的, 故

$$a_1^3=(ac^{\mp 1})^3=a^3c^{\mp 3}=b^{\pm 3}.$$

与 $\langle a_1\rangle\bigcap\langle b\rangle=1$ 矛盾. 于是 $|\langle a\rangle\bigcap H|=1$. 从而

$$|G|=|\langle a\rangle||H|=|\langle a\rangle||\langle b\rangle||\langle c\rangle|=3^{n+m+2}.$$

因此 $r=2$. 又 $n=2$, $m=2$, 故此时 G 的型不变量为 $(2,2,2)$.

由于 $c(G)\leqslant 3$, 下面分 $c(G)=2$ 和 $c(G)=3$ 两种情形讨论.

若 $c(G)=2$, 则 $G=\langle a,b,c \mid a^9=b^9=c^9=1,[a,b]=c,[c,a]=[c,b]=1\rangle$. 此为群 (3).

若 $c(G)=3$, 可设 $[c,a]=1$ 或 $[c,b]=1$. 这是因为, 若 $[c,a]\neq 1$ 且 $[c,b]\neq 1$. 由 $[c,a]\in Z(G)$, $[c,b]\in Z(G)$ 可得

$$[c,ab^i]=[c,a][c,b^i]=[c,a][c,b]^i.$$

又因 $[c,a]\in\langle c^3\rangle$, $[c,b]\in\langle c^3\rangle$, 故必存在 i 使得 $[c,ab^i]=1$. 由定理 13.1.1(7) 知 G 是 3^2 交换, 从而有

$$(ab^i)^{3^2}=a^{3^2}(b^i)^{3^2}=1,\quad o(ab^i)\leqslant o(a).$$

又由 $ab^i\in G\setminus L$, 令 $a_1=ab^i$. 则 a_1,b,d 还是 G 的一组唯一性基底, 且此时有 $[c,a_1]=1$ 成立.

若 $[c,b]=1$, 则 $[c,a]=c^3$ 或 $[c,a]=c^{-3}$.

当 $[c,a]=c^3$ 时, $G=\langle a,b,c \mid a^9=b^9=c^9=1,[a,b]=c,[c,a]=c^3,[c,b]=1\rangle$. 此为群 (4). 当 $[c,a]=c^{-3}$ 时, 用 a^{-1} 取代 a, 仍得到群 (4).

若 $[c,a]=1$, 则 $[c,b]=c^3$ 或 $[c,b]=c^{-3}$.

当 $[c,b]=c^3$ 时, 交换 a,b, 仍得到群 (4). 当 $[c,b]=c^{-3}$ 时, 用 b^{-1} 取代 a, 用 a 取代 b, 仍得到群 (4).

子情形 2.2　$n\geqslant 3$.

由定理 13.1.1(6) 知 $\mho_2(G)\leqslant Z(G)$, 从而有 $\langle a^{3^2}\rangle\leqslant Z(G)$. 又由定理 13.1.1(5) 知 $Z(G)$ 循环, 故可得 $\langle a^{3^2},c^3\rangle=\langle a^{3^2}\rangle$, 从而 $c^3\in\langle a^{3^2}\rangle\leqslant\langle a\rangle$, 即有 $c^3\in\langle a\rangle$, 故 $c^3=a^{\pm 3^{n-1}}$. 又由 $\langle a\rangle\bigcap\langle b\rangle=1$ 可得 $c^3\notin\langle b\rangle$, 从而 $\langle c\rangle\bigcap\langle b\rangle=1$.

$$|G|=|\langle a\rangle||\langle b,c\rangle|/|\langle a\rangle\bigcap\langle b,c\rangle|\leqslant|\langle a\rangle||\langle b\rangle||\langle c\rangle|/|\langle a^{3^{n-1}}\rangle|=3^{n+m+1},$$

从而 $r=1$. 故 G 的型不变量为 $(n,2,1)$.

当 $c(G)=2$ 时, $\langle a^9\rangle\langle c\rangle\leqslant Z(G)$, 由 $c\notin\langle a\rangle$ 且 $Z(G)$ 循环可得 $a^9=c^{\pm 3}$, 从而 $n\leqslant 3$. 故 $n=3$. 此时 G 的型不变量为 (3, 2, 1).

当 $a^9=c^3$ 时, 则

$$G=\langle a,b,c \mid a^{3^3}=b^{3^2}=1,c^3=a^{3^2},[a,b]=c,[c,a]=[c,b]=1\rangle.$$

此为群 (5). 当 $a^9=c^{-3}$ 时, 用 b^{-1} 取代 b, 仍得到群 (5).

当 $c(G)=3$ 时, 与子情形 2.1 类似, 仍可设 $[c,a]=1$ 或 $[c,b]=1$.

当 $[c,b]=1$ 时, 则 $[c,a]=c^3$ 或 $[c,a]=c^{-3}$.

当 $[c,a]=c^{-3}$ 时, 用 a^{-1} 取代 a, 则可转化为 $[c,a]=c^3$ 的情形. 故只需讨论 $[c,a]=c^3$ 的情形即可.

当 $[c,a]=c^3$ 时, $c^3=a^{3^{n-1}}$ 或 $c^3=a^{-3^{n-1}}$. 当 $c^3=a^{-3^{n-1}}$ 时, 用 b^{-1} 取代 b, 可转化为 $c^3=a^{3^{n-1}}$ 的情形. 故此时群 G 为

$$\langle a,b,c \mid a^{3^n}=b^{3^2}=1, c^3=a^{3^{n-1}}, [a,b]=c, [c,a]=c^3, [c,b]=1\rangle. \qquad (6)'$$

下证 $n=3$: 在群 $(6)'$ 中,

$$[c,a]=c^3,\quad [c,b]=1,\quad [a,b^3]=c^3,\quad [cb^3,a]=1,\quad [cb^3,b]=1,\quad cb^3\in Z(G).$$

故 $\langle cb^3,a^9\rangle$ 循环. 从而有 $\langle cb^3\rangle\leqslant\langle a^9\rangle$ 或 $\langle a^9\rangle<\langle cb^3\rangle$. 若 $\langle cb^3\rangle\leqslant\langle a^9\rangle$, 则 $cb^3=a^{9k}$, $c=a^{9k}b^{-3}$, 此时 $G'\leqslant \mho_1(G)$, 故 $\Phi(G)=\mho_1(G)$, 与 $\omega(G)=3$ 矛盾. 从而只能有 $\langle a^9\rangle<\langle cb^3\rangle$, 此时 $o(a^9)<o(cb^3)=3^2$, 从而 $n\leqslant 3$, 因此 $n=3$.

综上可得

$$G=\langle a,b,c \mid a^{3^3}=b^{3^2}=1, c^3=a^{3^2}, [a,b]=c, [c,a]=c^3, [c,b]=1\rangle.$$

我们得到群 (6).

当 $[c,a]=1$ 时, 则 $[c,b]=c^3$ 或 $[c,b]=c^{-3}$.

当 $[c,b]=c^3$ 时, 则

$$G=\langle a,b,c \mid a^{3^n}=b^{3^2}=1, c^3=a^{\pm 3^{n-1}}, [a,b]=c, [c,a]=1, [c,b]=c^3\rangle. \qquad (7)'$$

当 $[c,b]=c^{-3}$ 时, 用 a^{-1} 取代 a, b^{-1} 取代 b, 仍得到群 $(7)'$.

当 $c^3=a^{3^{n-1}}$ 时, 断言 $n\geqslant 4$. 若否, $n=3$, 从而 $(ca^{-3})^3=1$. 于是 $Z(G)\geqslant \langle a^9, ca^{-3}\rangle\cong C_3^2$. 这和 $Z(G)$ 循环矛盾. 这样就得到了群 (7) 和 (8).

定理中的群互不同构且皆为极小非 3 交换 3 群. 证明过程略去. □

定理 13.1.10 *设 G 为有限非正则 3 群且 $\exp(G)=3^e$. 则 G 为极小非 3 交换 3 群当且仅当 G 是下列互不同构群之一.*

(1) $G=\langle a,b,c \mid a^{3^e}=b^3=c^3=1, [a,b]=c, [a,c]=a^{3^{e-1}}, [b,c]=1\rangle$ $(e\geqslant 2)$;

(2) $G=\langle a,b,c \mid a^{3^e}=c^3=1, b^3=a^3, [a,b]=c, [a,c]=a^{3^{e-1}}, [b,c]=1\rangle$ $(e\geqslant 2)$;

(3) $G=\langle a,b,c \mid a^{3^e}=c^3=1, b^3=a^{-3}, [a,b]=c, [a,c]=a^{3^{e-1}}, [b,c]=1\rangle (e\geqslant 2)$;

(4) $G=\langle a,b,c \mid a^9=b^3=c^3=1, [a,b]=c, [a,c]=1, [b,c]=a^{-3}\rangle$.

证明 由题设条件知, G 为极小非正则 3 群. 由 [247] 中的定理 5.2.15 知 $d(G)=2$, 故可设 $G=\langle a,b\rangle$, 其中 $o(a)=3^e$. 由 [247] 中的定理 5.2.15 可得, $\mho_1(G)=Z(G)=\langle a^3\rangle$, 又由 [247] 中的定理 5.2.15 知 $\exp(G')\leqslant p$ 且 G/G' 为 $(3^{e-1},3)$ 型群, 因此 $b^3\in G'\bigcap\mho_1(G)=\langle a^{3^{e-1}}\rangle$, 从而有 $o(b)=3$ 或 9. 又由引理 13.1.4 知 $c(G)=3$, 故有 $G_3\leqslant G'\bigcap Z(G)=\langle a^{3^{e-1}}\rangle$, 从而有 $G_3=\langle a^{3^{e-1}}\rangle$.

注意 $e\geqslant 2$, 若 $o(b)=9$, 则有 $b^3=a^{s3^{e-1}}$, 其中 $(s,3)=1$. 当 $e>2$ 时, 令 $b_1=ba^{-s3^{e-2}}$, 则有 $b_1^3=b^3a^{-s3^{e-1}}=1$. 因此, 当 $e>2$ 时, 总存在生成元 b_1 使得

$o(b_1)=3$. 又由引理 13.1.8 可知, $|G|=3^{e+2}$. 下面我们分 $e=2$ 和 $e>2$ 两种情况进行讨论.

情形 1 $e=2$.

此时 $|G|=3^4$. 由 3^4 阶群的分类知, 满足上述条件的群有

(1) $G=\langle a,b,c \mid a^9=b^3=c^3=1,[a,b]=c,[a,c]=a^3,[b,c]=1\rangle$;

(2) $G=\langle a,b,c \mid a^9=c^3=1,b^3=a^3,[a,b]=c,[a,c]=a^3,[b,c]=1\rangle$;

(3) $G=\langle a,b,c \mid a^9=c^3=1,b^3=a^{-3},[a,b]=c,[a,c]=a^3,[b,c]=1\rangle$;

(4) $G=\langle a,b,c \mid a^9=b^3=c^3=1,[a,b]=c,[a,c]=1,[b,c]=a^{-3}\rangle$.

这 4 个群即为定理中的群 (1)—(4).

情形 2 $e>2$.

设 $[a,b]=c$. 由 [247] 中的定理 5.2.15 知, $\exp(G')=3$, 从而 $o(c)=3$. 因此 $c\notin\langle a\rangle$. 若否, 则有 $c\in\langle a^{3^{e-1}}\rangle\leqslant Z(G)$, 即 $G'\leqslant Z(G)$, $c(G)=2$, 与 $c(G)=3$ 矛盾. 又由 $G_3=\langle a^{3^{e-1}}\rangle$, 可设

$$[a,c]=a^{s3^{e-1}},\quad [b,c]=a^{t3^{e-1}},$$

其中 s,t 为 $0,1,-1$, 且不同时为 0.

若 $s=1$, $t=0$, 则 $G=\langle a,b,c \mid a^{3^e}=b^3=c^3=1,[a,b]=c,[a,c]=a^{3^{e-1}},[b,c]=1\rangle$. 此为群 (1).

若 $s=1$, $t\neq 0$, 则

$$G=\langle a,b,c \mid a^{3^e}=b^3=c^3=1,[a,b]=c,[a,c]=a^{3^{e-1}},[b,c]=a^{t3^{e-1}}\rangle.$$

令 $b_1=a^{-t}b$. 就有 $b_1^3=a^{-3t}b^3d$, 其中 $d\in\langle a^{-t},b\rangle'$, 因而

$$o(b_1)=3^e,\quad [a,b_1]=c,\quad [b_1,c]=1.$$

又因为 $b_1^3\in\mho_1(G)$, 所以 $b_1^3=a^{\pm 3}$. 此时我们分别得到群 (2) 和 (3).

若 $s=-1$, $t=0$, 令 $c_1=c^{-1}$, $b_1=b^{-1}$, 此时 G 同构于群 (1).

若 $s=-1$, $t\neq 0$, 令 $b_1=a^tb$. 则 $b_1^3=(a^tb)^3=a^{3t}b^3d$, 其中 $d\in\langle a^t,b\rangle'$. 因而

$$o(b_1)=3^e,\quad [a,b_1]=c,\quad [b_1,c]=1.$$

又因为 $b_1^3\in\mho_1(G)$, 所以 $b_1^3=a^{\pm 3}$. 再令 $c_2=c^{-1}$, $b_2=b_1^{-1}$, 则

$$b_2^3=a^{\mp 3},\quad [a,b_2]=c_2,\quad [a,c_2]=a^{3^{e-1}},\quad [b_2,c_2]=1.$$

此时 G 同构于群 (2) 或 (3).

当 $s=0$, $t\neq 0$ 时, 令 $a_1=ab^t$, $c_1=ca^{-3^{e-1}}$. 则

$$o(a_1)=3^e,\quad o(c_1)=3,\quad [a_1,b]=c_1,\quad [a_1,c_1]=a^{3^{e-1}},\quad [b,c_1]=a^{t3^{e-1}}.$$

再令 $b_2=a_1^{-t}b$, 则 $o(b_2)=3^e$, 因而

$$b_2^3=a_1^{\pm 3},\quad [a_1,b_2]=c_1,\quad [b_2,c_1]=1.$$

此时 G 同构于群 (2) 或 (3).

在群 (1)—(4) 中, 都有 $\mho_1(G')=1$ 成立. 若 G 正则, 则由 [244] 中的Ⅳ, 定理 2.4 知 G 是 3 交换群, 与它们是极小非 3 交换群矛盾. 故群 (1)—(4) 都是非正则的. 易证定理中的互不同构且皆为极小非 3 交换 3 群. □

13.2 极小非 $\mathcal{P}_2$-p 群的分类

有限群 G 称为一个**极小非 $\mathcal{P}_n$ 群**, 如果 G 的幂零类大于 n, 但是 G 的所有真子群和真商群的幂零类都不超过 n. 显然 $\mathcal{P}_n$ 群是幂零类不超过 n 的一个群类. 由文献 [144] 可知, 极小非 $\mathcal{P}_2$ 群的幂零类为 3. 这样的群已被文献 [206] 刻画并完全分类. 本节介绍这个分类结果.

首先给出极小非 $\mathcal{P}_2$ 群的某些性质及其刻画.

命题 13.2.1 (1) 设 G 是幂零类为 c 的群. 则

$$[a_1^{n_1},\cdots,a_c^{n_c}]=[a_1,\cdots,a_c]^{n_1\cdots n_c}.$$

(2) 设 G 是幂零类为 3 的群. 若 $p>2$, 则 $[a^p,b]=[a,b]^p[a,b,a]^{\binom{p}{2}}$. 若 $p=2$, 则 $[a^2,b]=[a,b]^2[a,b,a]$ 且 $[a^4,b]=[a,b]^4[a,b,a]^{\binom{4}{2}}$.

证明 由 [89] 中的Ⅲ, 引理 6.8 可得 (1). 直接计算可得 (2). □

命题 13.2.2 设 G 是极小非 $\mathcal{P}_2$ 群. 则

(1) $Z(G)$ 循环且 $|G_3|=p$;

(2) $[\Phi(G),G]\leqslant Z(G)$ 且 $\mho_1(G')\leqslant Z(G)$;

(3) $Z(G)\leqslant \Phi(G)$;

(4) $d(G)\leqslant 3$;

(5) 若 $d(G)=3$, 则 $p=3$ 且 G 是正则的. 进一步地, 设 $G=\langle a,b,c\rangle$. 则 $[a,b,c]=[b,c,a]=[c,a,b]\neq 1$.

证明 (1) 取 G 的一个 p 阶正规子群 N. 因为 $c(G/N)=2$, 故 $N=G_3$. 因而 G_3 是 G 的唯一的极小正规子群, 故 $Z(G)$ 循环.

(2) 因为 $\Phi(G)=G'\mho_1(G)$, 故 $[\Phi(G),G]=[G',G][\mho_1(G),G]$. 明显地, $[G',G]=G_3\leqslant Z(G)$. 取 $x,y,z\in G$. 由命题 13.2.1 可得, $[x^p,y,z]=1$ 且 $[x^p,y]\in Z(G)$. 注意到 $\mho_1(G)=\langle x^p\mid x\in G\rangle$. 故 $[\mho_1(G),G]\leqslant Z(G)$, 因而 $[\Phi(G),G]\leqslant Z(G)$.

若 $a\in G'$, $b\in G$, 则 $[a,b]\in G_3$. 因而 $[a^p,b]=[a,b]^p=1$. 即 $a^p\in Z(G)$. 所以 $\mho_1(G')\leqslant Z(G)$.

(3) 若否, 则存在 G 的一个生成元 $c\in Z(G)$. 因而存在 G 的极大子群 M 使得 $G=M\langle c\rangle$. 于是 $c(G)=c(H)\leqslant 2$, 矛盾. 故 $Z(G)\leqslant\Phi(G)$.

(4) 设 $d(G)\geqslant 4$. 对于 $a,b,c\in G$, 令 $H=\langle a,b,c\rangle$. 则 $H<G$ 且 $c(H)\leqslant 2$. 于是 $[a,b,c]=1$. 由此可得 $c(G)\leqslant 2$, 矛盾. 故 $d(G)\leqslant 3$.

(5) 因为 G 的任意一个二元生成子群均为类 2 的, 故 G 是正则的, 且满足 2-Engel 条件. 又 $c(G)=3$, 由 [89] 中的III, 定理 6.5 得 $p=3$. 令 $G=\langle a,b,c\rangle$. 因为

$$[a,bc,bc]=[a,b,b]=[a,c,c]=1,$$

有 $[a,b,c]=[c,a,b]$. 互换 a,b,c 的位置得

$$[a,b,c]=[c,a,b]=[b,c,a].$$

因为 $G_3\neq 1$, 故 $[a,b,c]=[b,c,a]=[c,a,b]\neq 1$. □

定理 13.2.3　设 G 是有限 p 群且 $d(G)=2$. 若 $Z(G)$ 循环且 $|G_3|=p$, 则 G 是极小非 $\mathcal{P}_2$ 群.

证明　因为 $Z(G)$ 循环, 所以 G_3 是 G 的唯一的极小正规子群. 因而 G 的每个真商群是类 2 的. 于是只需证 G 的每个真子群的类不超过 2 即可.

取 G 的一个极大子群 M. 则存在 $a\in H\backslash\Phi(G)$, $b\in G\backslash H$ 使得 $G=\langle a,b\rangle$. 很清楚, $H=\langle a,\Phi(G)\rangle$. 因而

$$H_3=\langle [x,y,z]\mid x,y,z\in\{a,G',\mho_1(G)\}\rangle.$$

若 x,y,z 中有一个属于 $\mho_1(G)$, 由命题 13.2.1 可得, $[x,y,z]=1$. 若不是这种情况, 则 x,y,z 中有一个属于 G', 我们也有 $[x,y,z]=1$. 因而 $H_3=1$, 即得所证. □

类似地, 我们也有如下定理.

定理 13.2.4　设 G 是有限 p 群且 $d(G)=3$. 若 $Z(G)$ 循环, $|G_3|=p$ 且 G 满足 2-Engel 条件, 则 G 是极小非 $\mathcal{P}_2$ 群.

定理 13.2.5　设 G 是极小非 $\mathcal{P}_2$ 群.

(1) 若 $d(G)=2$, 则 G' 循环或 $G'\cong \mathrm{C}_p^2$;

(2) 若 $d(G)=3$, 则 $G'\cong\mathrm{C}_3^4$ 或 $G'\cong\mathrm{C}_{3^m}\times\mathrm{C}_3^2$, 其中 $m>1$.

证明 (1) 设 $G=\langle a,b\rangle$. 则 $G'=\langle [a,b],G_3\rangle$. 因为 $c(G)=3$, 故 G' 交换. 若 $\mho_1(G')=1$, 则 $G'\cong \mathrm{C}_p^2$. 若 $\mho_1(G')\neq 1$, 注意到 G_3 是 G 的唯一的极小正规子群 G_3. 我们有 $G_3\leqslant \mho_1(G')\leqslant \Phi(G')$. 因而 $G'=\langle [a,b]\rangle$, 即 G' 循环.

(2) 设 $G=\langle a,b,c\rangle$. 由命题 13.2.2 可得, $[a,b,c]\neq 1$. 令 $N=\mho_1(G')G_3$. 把 $V=G'/N$ 看作为 $\mathrm{F}(p)$ 上的线性空间. 下证 $\dim V=3$. 若否, 设 $\dim V\leqslant 2$. 则 $[a,b]N,[b,c]N$ 和 $[c,a]N$ 是线性无关的. 不妨设

$$[a,b]N=[b,c]^iN[c,a]^jN.$$

所以 $[a,b]\equiv [b,c]^i[c,a]^j \pmod N$. 由 $N\leqslant Z(G)$ 推出

$$[a,b,c]=[[b,c]^i[c,a]^j,c]=1.$$

矛盾. 故 $\dim V=3$. 其次, 若 $\mho_1(G')=1$, 则 $|G'/G_3|=3^3$. 因而 $|G'|=3^4$ 且 $G'\cong \mathrm{C}_3^4$. 若 $\mho_1(G')\neq 1$, 由 $G_3\leqslant \mho_1(G')$ 推出 $|G'/\mho_1(G')|=3^3$. 令 $\exp(G')=3^m$. 则 $m>1$. 因为 $\mho_1(G')\leqslant Z(G)$ 循环, 故 $G'\cong \mathrm{C}_{3^m}\times \mathrm{C}_3^2$. □

下面分类极小非 $\mathcal{P}_2$ 群. 注意到, 若 G 是 p^4 阶的极小非 $\mathcal{P}_2$ 群, 则 G 是极大类的. 下设 $|G|\geqslant p^5$. 由命题 13.2.2(4), $d(G)\leqslant 3$. 故只需分 $d(G)=2$ 和 $d(G)=3$ 两种情况讨论.

定理 13.2.6 设 G 是二元生成的亚循环的极小非 $\mathcal{P}_2$ 群. 则 G 与下列群同构:

$$\langle a,b\mid a^{p^{2r+1}}=1,\ b^{p^{r+t+1}}=a^{p^{r+1}},\ a^b=a^{1+p^r}\rangle,$$

其中 $r\geqslant 1$, $t\geqslant 0$. G 是可裂的当且仅当 $p>2$ 且 $t=0$, 或 $p=2$, $r\geqslant 2$, $t=0$.

证明 检查定理 6.1.3 和定理 6.1.4 即得. □

定理 13.2.7 设 G 是二元生成的非亚循环的极小非 $\mathcal{P}_2$ 群. 若 G' 循环, 则 G 同构于下列互不同构的群之一.

(I) $\langle a,b\mid a^{2^n}=c^{2s},b^2=c^4=1,[a,b]=c,[c,a]=1,[c,b]=c^2\rangle$, 当 $n=2$ 时, $s=0$; 当 $n>2$ 时, $s=1$.

(II) $\langle a,b\mid a^{p^n}=1,b^{p^n}=c^{p^v},c^{p^n}=1,[a,b]=c,[c,a]=1,[c,b]=c^{p^{n-1}}\rangle$, $v=1,2,\cdots,n$, $n\geqslant 2$, $v\neq n$, 当 $p=2$ 时, $n>2$.

(III) $\langle a,b\mid a^{2^n}=b^{2^n}=c^{2^{n-1}},c^{2^n}=1,[a,b]=c,[c,a]=1,[c,b]=c^{2^{n-1}}\rangle$, $n>2$.

(IV) $\langle a,b\mid a^{p^n}=c^{p^u},b^{p^m}=c^{p^m}=1,[a,b]=c,[c,a]=1,[c,b]=c^{sp^{m-1}}\rangle$, $n\geqslant m\geqslant 2$, $s=1,2,\cdots,p-1$, 当 $p=2$ 时, $m>2$, 当 $n>m$ 时, $u=1$. 当 $n=m$ 时, $u=1,2,\cdots,n-1$ 且 $s\neq 1$ 或 $u\neq 1$. 反之, 定理中群均为极小非 $\mathcal{P}_2$ 群.

证明 因为 $d(G)=2$ 且 G' 循环, 故 $\overline{G}=G/\mho_1(G')$ 是内交换的. 又 G 非亚循环, 由定理 2.5.3 知, $\overline{G}$ 非亚循环. 由定理 1.7.10 可设

$$\overline{G}=\langle \bar{a},\bar{b},\bar{c}\mid \bar{a}^{p^n}=\bar{b}^{p^m}=\bar{c}^p=\bar{1},[\bar{a},\bar{b}]=\bar{c},[\bar{c},\bar{a}]=[\bar{c},\bar{b}]=\bar{1}\rangle,$$

其中 $n \geqslant m$, 若 $p=2$, 则 $n+m \geqslant 3$. 令 a,b,c 分别是 $\bar{a},\bar{b},\bar{c}$ 的在自然同态下的一个原像. 则 $G=\langle a,b,c\rangle$. 因为 $G'=\langle c\rangle$, 不妨设 $[a,b]=c$ 且 $o(c)=p^r$, 其中 $r \geqslant 2$. 计算可得, $r \leqslant m$ 除非 $p=2$, $r=2$, $m=1$. 因为 $|G_3|=p$, 所以 $[c,a]$ 与 $[c,b]$ 中至少有一个不为 1. 断言: $[c,b] \neq 1$. 若否, 如果 $n=m$, 在必要的情况下, 互换 a, b 的位置就有 $[c,b]\neq 1$. 如果 $n>m$, 设 $[c,b]=1$, 则令 $[c,a]=c^{ip^{r-1}}$, 其中 $p \nmid i$. 计算可得, $a^{p^r}, b^{ip^{r-1}}c \in Z(G)$. 所以 $\bar{a}^{p^r}, \overline{b^{ip^{r-1}}c} \in Z(G)/\mho_1(G')$. 注意到 $Z(G)$ 循环, 故 $Z(G)/\mho_1(G')$ 也循环. 因为 $o(\bar{a}^{p^r}) \geqslant o(\overline{b^{ip^{r-1}}c})$, 所以 $\overline{b^{ip^{r-1}}c}=\bar{1}$. 矛盾. 故 $[c,b]\neq 1$. 所以在必要的情况下, 作生成元替换, 可设

$$a^{p^n}=c^{p^u},\quad b^{p^m}=c^{p^v},\quad [c,a]=1,\quad [c,b]=c^{sp^{r-1}},$$

其中 $1 \leqslant u,v \leqslant r$, $n \geqslant m$, $p \nmid s$.

通过计算, 有

$$Z(G)=\begin{cases}\langle a^{-2}c, a^4, b^2\rangle, & |G'|=2^2,\\ \langle a^{-sp^{r-1}}c, a^{p^r}, b^{p^r}\rangle, & p>2 \text{ 或 } p=2 \text{ 且 } |G'|>2^2.\end{cases}$$

情形 1　$|G'|=2^2$.

注意到 $Z(G)$ 循环. 故 $Z(G)/\mho_1(G')=\langle\overline{a^{-2}c}, \bar{a}^4, \bar{b}^2\rangle$ 也循环. 注意到 $\bar{a}^4=(\overline{a^{-2}c})^2$ 且 $\overline{a^{-2}c}\neq\bar{1}$. 因为 $\langle\overline{a^{-2}c}\rangle\bigcap\langle\bar{b}\rangle=\bar{1}$, 故 $\bar{b}^2=\bar{1}$. 从而 $m=1$. 于是 $Z(G)=\langle a^{-2}c, c^2\rangle$. 又 $o(a^{-2}c)>o(c^2)=2$, 故 $Z(G)=\langle a^{-2}c\rangle$.

明显地, $(a^{-2}c)^{2^{n-1}}=c^{-2^u+2^{n-1}}$. 若 $n=2$, 则 $(a^{-2}c)^2=c^{2(1-2^{u-1})}$. 因为 $o(a^{-2}c)>2$, 故 $u=2$. 因而 $a^4=1$. 若 $n>2$, 则可证 $u=1$. 注意到 $b^2=c^{2^v}$. 若 $v=1$, 令 $b_1=ba^{-2^{n-1}}$. 则 $b_1^2=1$. 故不妨设 $b^2=1$. 我们得到群 (Ⅰ).

情形 2　$p>2$ 或 $p=2$ 且 $|G'|>2^2$.

类似于情形 1 的论证, 由 $Z(G)$ 循环, 有

$$\bar{b}^{p^r}=1,\quad Z(G)/\mho_1(G')=\langle\overline{a^{-sp^{r-1}}c}\rangle.$$

由 $\bar{b}^{p^r}=1$ 可得 $m \leqslant r$. 若 $p=2$, 我们断言 $m \geqslant 2$. 若否, 有

$$1=[a,b^2]=c^{2(1+2^{r-2})}.$$

因为 $r>2$, 故 $c^2=1$, 矛盾. 由命题 13.2.1 可得, $1=[a,b^{p^m}]=c^{p^m}$. 于是 $m=r$. 从而当 $p=2$ 时, $2 \leqslant m \leqslant n$ 且 $m>2$.

(i) 若 $n=m$, 我们断言 $(a^{-sp^{n-1}}c)^p \neq 1$. 若否, $a^{-sp^{n-1}}c \in \mho_1(G')$. 于是 $\overline{a^{-sp^{n-1}}c}=\bar{1}$, 矛盾. 因为

$$1 \neq (a^{-sp^{n-1}}c)^p=c^{p(1-sp^{u-1})},$$

故 $s \neq 1$ 或 $u \neq 1$ 且 $c^p \in \langle a^{-sp^{n-1}}c\rangle$. 因而 $Z(G) = \langle a^{-sp^{n-1}}c\rangle$.

若 $u > v$, 令

$$a_1 = ab^{-p^{u-v}}, \quad b_1 = b^k, \quad c_1 = [a_1, b_1] \equiv c^k (\mathrm{mod}\ G_3),$$

其中 $sk \equiv 1(\mathrm{mod}\ p)$. 我们有

$$a_1^{p^n} = 1, \quad b_1^{p^n} = c_1^{p^v}, \quad [c_1, a_1] = 1, \quad [c_1, b_1] = c_1^{p^{n-1}}.$$

我们得到群 (Ⅱ), 其中 $1 \leqslant v \leqslant n-1$.

若 $u \leqslant v$, 当 $p > 2$ 且 $u = n$ 时, 明显地, $v = n$. 用 b^k 替换 b, 其中 $sk \equiv 1(\mathrm{mod}\ p)$, 得到群 (Ⅱ), 其中 $v = n$. 当 $p > 2$ 且 $u \neq n$ 或 $p = 2$ 且 $u < v$ 时, 用 $ba^{-p^{v-u}}$ 替换 b 有 $b^{p^n} = 1$. 此时得到群 (Ⅳ), 其中 $n = m$. 若 $p = 2$ 且 $u = v$, 用 ba^{-1} 替换 b 有 $b^{2^n} = c^{2^{n-1}}$. 这说明当 $u = n$ 时, 这归结为 $u > v$ 的情形. 若 $u < n-1$, 归结为 $u < v = n-1$ 的情形. 因而可设 $u = n-1$. 这就得到群 (Ⅲ).

(ii) 设 $n > m$. 因为 $a^{p^{n-1}} \in Z(G) \backslash \mho_1(G')$, 有 $o(a^{p^{n-1}}) > p^{m-1}$. 故 $o(a^{p^n}) \geqslant p^{m-1}$. 又因为 $o(a^{p^n}) = p^{m-u}$, 故得 $u = 1$. 故 $a^{p^n} = c^p$. 由此可得

$$(a^{-sp^{m-1}}c)^{p^{n-m+1}} = c^{p(-s+p^{n-m})}.$$

因为 $p \nmid (-s + p^{n-m})$, 有 $c^p \in \langle a^{-sp^{m-1}}c\rangle$. 从而 $Z(G) = \langle a^{-sp^{m-1}}c\rangle$. 令

$$b_1 = ba^{-p^{n-m+v-1}}.$$

则

$$b_1^{p^m} = 1, \quad [a, b_1] = c, \quad [c, a] = 1, \quad [c, b_1] = c^{sp^{m-1}}.$$

此时 G 同构于群 (Ⅳ), 其中 $n > m$.

反之, 对定理中的每个群, 不难证明, 均有 $|G_3| = p$ 且 $Z(G)$ 循环. 由定理 13.2.3 可知, 它们均为极小非 $\mathcal{P}_2$ 群.

下证定理中的群互不同构. 先证对于群 (Ⅱ) 与 (Ⅳ) 来说, 不同的参数给出不同构的群. 对于群 (Ⅱ) 来说, 因为 $\exp(G) = p^{2n-v}$, 显然, v 的不同值给出的群不同构. 对 (Ⅳ) 来说, 为简便起见, 用 $G(u, s)$ 表示群 (Ⅳ). 因为 $\exp(G) = p^{n+m-u}$, 显然, u 的不同值给出的群不同构. 再证, s 的不同值给出的群不同构. 若 $p = 2$, 则 $s = 1$. 不妨设 $p > 2$, $G(u, s_1) \cong G(u, s_2)$, 其中 $s_1, s_2 \in \{1, \cdots, p-1\}$. 对于 $G(u, s_1)$, 令

$$a_2 = a^{i_1}b^{j_1}c^{k_1}, \quad b_2 = a^{i_2p^{n-u}}b^{j_2}c^{k_2},$$

其中 $i_1, i_2, j_1, j_2, k_1, k_2$ 满足 $p \nmid i_1$ 且 $p \nmid j_2$ 并使得 a_2, b_2 是 $G(u, s_1)$ 的一组生成元, 且 $a_2, b_2, c_2 = [a_2, b_2]$ 满足 $G(u, s_2)$ 的定义关系. 计算可得

$$i_1p^u \equiv i_1j_2p^u (\mathrm{mod}\ p^m), \quad s_1i_1j_2^2 \equiv s_2i_1j_2 (\mathrm{mod}\ p).$$

于是 $s_1 \equiv s_2 (\bmod p)$, 即 $s_1 = s_2$.

下证群 (Ⅱ)—(Ⅳ) 互不同构. 我们观察到, 对于群 (Ⅱ) 和 (Ⅲ), $G/\mho_1(G') \cong \mathrm{M}_p(n,n,1)$. 对于群 (Ⅳ), $G/\mho_1(G') \cong \mathrm{M}_p(n,m,1)$. 故当 $n > m$ 时, 群 (Ⅳ) 与群 (Ⅱ) 和 (Ⅲ) 均不同构. 设 $n = m$. 对于群 (Ⅱ),

$$\exp(G) = p^{2n-v}, \quad \exp(C_G(G')) = p^{2n-v-1}.$$

对于群 (Ⅲ),

$$\exp(G) = \exp(C_G(G')) = 2^{n+1},$$

而对于群 (Ⅳ),

$$\exp(G) = \exp(C_G(G')) = p^{2n-u}.$$

因而群 (Ⅱ) 与群 (Ⅲ) 和 (Ⅳ) 均不同构. 若 $p = 2$, 对于群 (Ⅲ) 和 (Ⅳ) 来说, 若 $u < n-1$, 则它们的方次数不相等. 若 $u = n-1$, 则它们的 2^n 阶元的个数不相等. 故群 (Ⅲ) 和 (Ⅳ) 互不同构. □

定理 13.2.8 *设 G 是二元生成的非亚循环的极小非 $\mathcal{P}_2$ 群. 若 $G' \cong \mathrm{C}_p^2$, 则 G 同构于下列互不同构的群之一.*

(Ⅰ) $\langle a,b \mid a^{p^{n+1}} = b^p = c^p = 1, [a,b] = c, [c,a] = 1, [c,b] = a^{up^n}\rangle$, $p > 2$, $n \geqslant 2$, $u = 1$ 或 ν, ν 是一个固定的模 p 的平方非剩余;

(Ⅱ) $\langle a,b \mid a^{p^{n+1}} = b^p = c^p = 1, [a,b] = c, [c,a] = a^{p^n}, [c,b] = 1\rangle$, $p > 2$, $n \geqslant 2$;

(Ⅲ) $\langle a,b \mid a^{2^{n+1}} = b^4 = c^2 = 1, [a,b] = c, [c,a] = 1, [c,b] = a^{2^n}\rangle$, $n \geqslant 1$;

(Ⅳ) $\langle a,b \mid a^{2^{n+1}} = b^2 = c^2 = 1, [a,b] = c, [c,a] = a^{2^n}, [c,b] = 1\rangle$, $n \geqslant 2$;

(Ⅴ) $\langle a,b \mid a^8 = 1, b^2 = a^4, c^2 = 1, [a,b] = c, [c,a] = a^4, [c,b] = 1\rangle$.

反之, 定理中群均为极小非 $\mathcal{P}_2$ 群.

证明 因为 $d(G) = 2$ 且 $G' \cong \mathrm{C}_p^2$, 由定理 1.7.7 可知, G/G_3 内交换. 又 G 非亚循环, 由定理 2.5.3 知, $\overline{G}$ 非亚循环. 再由定理 1.7.10 可设

$$G/G_3 = \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^n} = \bar{b}^{p^m} = \bar{c}^p = \bar{1}, [\bar{a},\bar{b}] = \bar{c}, [\bar{c},\bar{a}] = [\bar{c},\bar{b}] = \bar{1}\rangle,$$

其中 $n \geqslant m$, 且当 $p = 2$ 时, $n + m \geqslant 3$. 令 a, b, c 分别是 $\bar{a}, \bar{b}, \bar{c}$ 的在自然同态下的一个原像. 则 $G = \langle a, b, c\rangle$. 不妨设 $[a,b] = c$. 则 $G' = \langle c\rangle \times G_3$. 进一步地, 因为 $|G| \geqslant p^5$, 故 $n \geqslant 2$.

情形 1 $p > 2$.

因为 $\exp(G') = p$, 由命题 13.2.1 可得, $a^p, b^p \in Z(G)$, 所以 $\bar{a}^p, \bar{b}^p \in Z(G)/G_3$. 因为 $Z(G)$ 循环且 $G_3 \leqslant Z(G)$, 有 $\langle a^{o(a)/p}\rangle = G_3$, 故 $\bar{a}^{o(a)/p} = \bar{1} \in G/G_3$. 于是 $p^n = o(\bar{a}) \leqslant o(a)/p$. 由此可得, $o(a) = p^{n+1}$ 且 $G_3 = \langle a^{p^n}\rangle$. 又因为 $Z(G)/G_3$ 循环, 有 $m = 1$ 且 $b^p \in G_3$. 令 $b^p = a^{ip^n}$. 用 $ba^{-ip^{n-1}}$ 替换 b, 不妨设 $b^p = 1$.

因为 $c(G)=3$, 所以 $[c,a]$ 与 $[c,b]$ 至少有一个不等于 1. 不妨设 $[c,b]\neq 1$. 进一步可设 $[c,b]=a^{ip^n}$, 其中 $p\nmid i$. 令 $[c,a]=a^{jp^n}$. 用 $a_1=ab^{-i^{-1}j}$ 替换 a, 则 $[c,a_1]=1$. 用 $b_1=b^k$ 替换 b, $c_1=[a_1,b_1]$ 替换 c, 有 $[c_1,a_1]=1$, $[c_1,b_1]=a_1^{ik^2p^n}$. 设 ν 是一个固定的模 p 的平方非剩余, 则 G 同构于下列群之一:

(1) $\langle a,b \mid a^{p^{n+1}}=b^p=c^p=1,[a,b]=c,[c,a]=1,[c,b]=a^{p^n}\rangle$;

(2) $\langle a,b \mid a^{p^{n+1}}=b^p=c^p=1,[a,b]=c,[c,a]=1,[c,b]=a^{\nu p^n}\rangle$.

我们得到群 (I).

设 $[c,b]=1$. 则 $[c,a]\neq 1$. 令 $[c,a]=a^{ip^n}$, 其中 $p\nmid i$. 记 $b_1=b^k$, 其中 $ik\equiv 1(\bmod p)$, $c_1=[a,b_1]$. 则 $[c_1,b_1]=1$, $[c_1,a]=a^{p^n}$. 我们得到群 (II).

情形 2 $p=2$.

与情形 1 的证明类似, 有 $a^4,b^4\in Z(G)$ 且 $\bar{a}^4,\bar{b}^4\in Z(G)/G_3$. 故 $\bar{b}^4=\bar{1}$. 从而 $m\leqslant 2$. 不难证明: $[c,a]$ 和 $[c,b]$ 中至少有一个为 1.

设 $[c,a]=1$. 由命题 13.2.1 可得, $a^2\in Z(G)$. 因为 $Z(G)$ 循环且 $G_3\leqslant Z(G)$, 故 $\langle a^{o(a)/2}\rangle=G_3$. 从而 $\bar{a}^{o(a)/2}=\bar{1}\in G/G_3$. 于是 $2^n=o(\bar{a})\leqslant o(a)/2$. 由此可得 $o(a)=2^{n+1}$ 且 $G_3=\langle a^{2^n}\rangle$. 因为 $b^{2^m}\in G_3$, 故 $b^{2^m}=a^{i2^n}$. 用 $b_1=ba^{-i2^{n-m}}$ 替换 b, 有 $b_1^{2^m}=1$. 因为 $[a,b_1^2]=[c,b_1]\neq 1$, 故 $b_1^2\neq 1$. 因而 $m=2$. 得到群 (III), 其中 $n\geqslant 2$.

设 $[c,b]=1$. 此时不妨设 $n>m$. 若 $n\geqslant 3$, 由于 $a^4\in Z(G)$ 且 $Z(G)$ 循环, 与上段的论证类似, 可得 $G_3=\langle a^{2^n}\rangle$, $o(a)=2^{n+1}$. 注意到 $b^{2^m}\in G_3$. 不妨设 $b^{2^m}=1$. 断言 $m=1$. 若否, $m=2$. 因为 $[c,b]=1$, 由命题 13.2.1 可得, $b^2\in Z(G)$. 因而 $\langle b^2\rangle=G_3$, $\bar{b}^2=\bar{1}$, 矛盾. 此时得到群 (IV), 其中 $n\geqslant 3$. 下设 $n=2$. 此时 $m=1$ 且 $b^2\in G_3$, $o(b)\leqslant 4$. 注意到 $a^4\in Z(G)$. 若 $a^4\neq 1$. 我们有 $G_3=\langle a^4\rangle$. 从而 $b^2=1$ 或 $b^2=a^4$. 得到群 (IV), 其中 $n=2$, 或群 (V). 若 $a^4=1$. 则 $o(b)=4$ 或 $o(b)=2$. 若 $o(b)=4$, 则 $G_3=\langle b^2\rangle$. 互换 a 与 b 的位置, 得到群 (III), 其中 $n=1$. 若 $o(b)=2$, 用 a^2b 替换 a , 用 a 替换 b, 也得到群 (III), 其中 $n=1$.

类似于定理 13.2.7 的证明方法, 可证定理中的群互不同构且均为极小非 $\mathcal{P}_2$ 群. 证明的细节在此略去. □

下面处理 $d(G)=3$ 的情况. 由定理 13.2.5, 有 $G'\cong \mathrm{C}_3^4$ 或 $G'\cong \mathrm{C}_{3^m}\times \mathrm{C}_3^2$, 其中 $m>1$.

定理 13.2.9 设 G 是三元生成的极小非 $\mathcal{P}_2$ 群. 若 $G'\cong \mathrm{C}_3^4$, 则 G 同构于下列互不同构的群之一.

(I) $\langle a,b,c \mid a^3=b^3=c^3=d_1^3=d_2^3=d_3^3=d_4^3=1,[a,b]=d_1,[b,c]=d_2,[c,a]=d_3,[d_1,c]=[d_2,a]=[d_3,b]=d_4,[d_1,a]=[d_1,b]=[d_2,b]=[d_2,c]=[d_3,a]=[d_3,c]=1,d_4\in Z(G)\rangle$;

(II) $\langle a,b,c \mid a^{3^e}=b^3=c^3=d_1^3=d_2^3=d_3^3=1,[a,b]=d_1,[b,c]=d_2,[c,a]=$

$d_3, [d_1, c] = [d_2, a] = [d_3, b] = a^{3^{e-1}}, [d_1, a] = [d_1, b] = [d_2, b] = [d_2, c] = [d_3, a] = [d_3, c] = 1\rangle$, $e \geqslant 2$.

反之, 定理中群均为极小非 $\mathcal{P}_2$ 群.

证明 令 $G = \langle a, b, c\rangle$ 且 $o(a) \geqslant o(b) \geqslant o(c)$. 因为 $G' \cong \mathrm{C}_3^4$, 不妨设

$$G' = \langle [a, b]\rangle \times \langle [b, c]\rangle \times \langle [c, a]\rangle \times G_3.$$

若 $\exp(G) = 3$, 则 $\Phi(G) = G'$. 因为 $|G/\Phi(G)| = 3^3$ 且 $|G'| = 3^4$, 有 $|G| = 3^7$. 记

$$[a, b] = d_1, \quad [b, c] = d_2, \quad [c, a] = d_3.$$

由命题 13.2.2(5), 不妨设

$$[a, b, c] = [b, c, a] = [c, a, b] = d_4.$$

此时得到群 (Ⅰ).

设 $\exp(G) = 3^e > 3$. 因为 $\exp(G') = 3$, 由命题 13.2.1 可得, $a^3, b^3, c^3 \in Z(G)$. 于是对适当的 i, j, 不妨设 $b^3 = a^{3i}$, $c^3 = a^{3j}$. 分别用 ba^{-i} 和 ca^{-j} 替换 b 和 c, 可得 $b^3 = c^3 = 1$. 因为 G 正则, 故 $o(a) = 3^e$. 由此可得 $Z(G) = \langle a^3\rangle$, $G_3 = \langle a^{3^{e-1}}\rangle$. 由命题 13.2.2(5), 不妨设

$$[a, b, c] = [b, c, a] = [c, a, b] = a^{3^{e-1}}.$$

必要的情况下, 用 c 的适当的幂替换 c, 记

$$[a, b] = d_1, \quad [b, c] = d_2, \quad [c, a] = d_3.$$

得到群 (Ⅱ). □

定理 13.2.10 *设 G 是三元生成的极小非 $\mathcal{P}_2$ 群. 若 $G' \cong \mathrm{C}_{3^m} \times \mathrm{C}_3^2$, 其中 $m > 1$, 则 G 同构于下列互不同构的群之一.*

(Ⅰ) $\langle a, b, c \mid b^{3^m} = c^3 = d^{3^m} = e^3 = 1, a^{3^{m+u}} = d^3, [a, b] = d, [b, c] = b^{-3^{m-1}}, [c, a] = e, [d, c] = [e, b] = d^{3^{m-1}}, [d, a] = [d, b] = [e, a] = [e, c] = 1\rangle$, $u \geqslant 0$;

(Ⅱ) $\langle a, b, c \mid b^{3^m} = d^{3^m} = 1, a^{3^{m+u}} = d^3, c^{3^v} = a^{3^m}, [a, b] = d, [b, c] = b^{-3^{m-1}}, [c, a] = a^{3^{m-1}} c^{-3^{v-1}}, [d, c] = d^{3^{m-1}}, [d, a] = [d, b] = 1\rangle$, $u \geqslant 0$, $1 < v < m$;

(Ⅲ) $\langle a, b, c \mid b^{3^m} = c^3 = d^{3^m} = 1, a^{3^m} = d^{3^u}, [a, b] = d, [b, c] = b^{-3^{m-1}}, [c, a] = a^{3^{m-1}} d^{-3^{u-1}}, [d, c] = d^{3^{m-1}}, [d, a] = [d, b] = 1\rangle$, $1 < u \leqslant m$;

(Ⅳ) $\langle a, b, c \mid b^{3^m} = d^{3^m} = 1, a^{3^m} = d^{3^u}, c^{3^v} = d^3, [a, b] = d, [b, c] = b^{-3^{m-1}}, [c, a] = a^{3^{m-1}} d^{-3^{u-1}}, [d, c] = d^{3^{m-1}}, [d, a] = [d, b] = 1\rangle$, $1 < u < m-1$, $1 < v < m-u+1$;

(V) $\langle a,b,c \mid a^{3^m}=b^{3^m}=d^{3^m}=1, c^{3^v}=d^3, [a,b]=d, [b,c]=b^{-3^{m-1}}, [c,a]=a^{3^{m-1}}, [d,c]=d^{3^{m-1}}, [d,a]=[d,b]=1\rangle$, $v>1$.

反之, 定理中群均为极小非 $\mathcal{P}_2$ 群.

证明 令 $G=\langle a,b,c\rangle$. 因为 G 是极小非 $\mathcal{P}_2$ 群, 由命题 13.2.2 可知, $Z(G)$ 循环且 $G_3\leqslant \mho_1(G')\leqslant Z(G)$. 于是

$$G'=\langle [a,b],[b,c],[c,a],G_3\rangle=\langle [a,b],[b,c],[c,a]\rangle,\quad [a,b]^3,\ [b,c]^3,\ [c,a]^3\in Z(G).$$

因为 $Z(G)$ 循环且 $\exp(G')=3^m$, 所以对适当的 i,j, 不妨设

$$o([a,b])=3^m,\quad o(a)\geqslant o(b),\quad [b,c]^3=[a,b]^{3i},\quad [c,a]^3=[a,b]^{3j}.$$

令 $c_1=ca^ib^j$. 则

$$[b,c_1]\equiv [b,c][b,a]^i (\bmod G_3),\quad [c_1,a]\equiv [c,a][b,a]^j (\bmod G_3).$$

于是不妨设

$$o([b,c])=o([c,a])=3,\quad G'=\langle [a,b]\rangle\times\langle [b,c]\rangle\times\langle [c,a]\rangle.$$

记 $[a,b]=d$. 则 $G_3=\langle d^{3^{m-1}}\rangle$. 必要的情况下, 用 c 的适当的幂替换 c, 再由命题 13.2.2(5), 不妨设

$$[a,b,c]=[b,c,a]=[c,a,b]=d^{3^{m-1}}.$$

因为 $\exp(G')=3^m$, 由命题 13.2.1 可得, $a^{3^m},b^{3^m}\in Z(G)$. 于是对某个整数 i 可设 $b^{3^m}=a^{i3^m}$. 用 ba^{-i} 替换 b, 有 $b^{3^m}=1$. 计算可得

$$b^{3^{m-1}}[b,c]\in Z(G),\quad (b^{3^{m-1}}[b,c])^3=1.$$

于是对某个整数 j, $b^{3^{m-1}}[b,c]=d^{j3^{m-1}}$. 由此可得 $[b,c]=b^{-3^{m-1}}d^{j3^{m-1}}$. 用 $c[c,a]^j$ 替换 c, 有 $[b,c]=b^{-3^{m-1}}$. 因为 G 正则, 由 $o([b,c])=o([c,a])=3$ 易得 $c^3\in Z(G)$. 若 $o(c)\leqslant 3^m$, 对某个整数 i 可设 $c^3=d^{3i}$. 用 cd^{-i} 替换 c 可得 $c^3=1$. 现在得到 $o(c)=3$ 或 $o(c)>3^m$. 又因为 $Z(G)$ 循环且 $a^{3^m},d^3\in Z(G)$, 又有 $\langle a^{3^m}\rangle\geqslant\langle d^3\rangle$ 或 $\langle d^3\rangle>\langle a^{3^m}\rangle$.

情形 1 $\langle a^{3^m}\rangle\geqslant\langle d^3\rangle$.

令 $d^3=a^{l3^{m+u}}$, 其中 $3\nmid l$, $u\geqslant 0$. 则 $o(a)=3^{2m+u-1}$. 分别用 b 和 d 的适当幂替换 b 和 d, 有 $a^{3^{m+u}}=d^3$, $u\geqslant 0$, 且仍然有

$$b^{3^m}=d^{3^m}=1,\quad [a,b]=d,\quad [b,c]=b^{-3^{m-1}},\quad [a,b,c]=[b,c,a]=[c,a,b]=d^{3^{m-1}}.$$

因为

$$[d,c]\neq 1,\quad [a^3,c]=[a,c]^3=1,\quad d\notin\langle a^3\rangle,\quad [d,a]=1,$$

有 $\langle a,d\rangle\cong C_{3^{2m+u-1}}\times C_3$. 又因为 $[b^{3^{m-1}},a]\neq 1$, 故 $b^{3^{m-1}}\notin\langle a,d\rangle$. 注意到 $b\in N_G(\langle a,d\rangle)$ 且 $o(b)=3^m$, 有

$$\langle a,b\rangle=\langle a,d\rangle\rtimes\langle b\rangle,\quad |\langle a,b\rangle|=3^{3m+u}.$$

记 $[c,a]=e$. 断言 $e\notin\langle a,b\rangle$. 若否, $e\in\langle a,b\rangle$. 因为 $o(e)=3$, 故

$$e\in\Omega_1(\langle a,b\rangle)=\Omega_1(\langle a,d\rangle)\times\langle b^{3^{m-1}}\rangle.$$

由此得 $[e,b]=1$, 矛盾. 于是

$$\langle a,b,e\rangle=\langle a,b\rangle\rtimes\langle e\rangle,\quad |\langle a,b,e\rangle|=3^{3m+u+1}.$$

(i) 若 $c^3=1$, 则

$$G=\langle a,b,e\rangle\rtimes\langle c\rangle,\quad |G|=3^{3m+u+2},\quad \exp(G)=3^{2m+u-1}.$$

此时我们得到群 (I), 且不同的参数 u 对应的群是不同构的.

(ii) 若 $o(c)>3^m$, 断言 $o(a)>o(c)$. 若否, 因为 $a^{3^m},c^3\in Z(G)$, 故 $a^{3^m}\in\langle c^{3^m}\rangle$. 于是对某个整数 i, $a^{3^m}=c^{i3^m}$. 用 ac^{-i} 替换 a 可得, $a^{3^m}=1$, 矛盾.

因为 $a^{3^m},c^3\in Z(G)$, 故 $\langle a^{3^m}\rangle<\langle c^3\rangle$ 或 $\langle a^{3^m}\rangle\geqslant\langle c^3\rangle$. 若后者成立, 则 $c^3=a^{i3^m}$ 且 $(ca^{-i3^{m-1}}[c,a]^i)^3=1$. 用 $ca^{-i3^{m-1}}[c,a]^i$ 替换 c, 有

$$c^3=[b,c]^3=[c,a]^3=1,\quad [b,c]=b^{-3^{m-1}}.$$

这归结到情形 (i). 下设 $\langle a^{3^m}\rangle<\langle c^3\rangle$. 于是对满足 $3\nmid i$ 和 $v>1$ 的整数 i,v 有 $a^{3^m}=c^{i3^v}$. 由此可得 $o(c)=3^{m+u+v-1}$. 分别用 a 和 d 的适当幂替换 a 和 d, 有 $a^{3^m}=c^{3^v}$. 因为

$$o(a)=3^{2m+u-1}>o(c)=3^{m+u+v-1},$$

故 $m>v$. 通过简单的计算可得

$$a^{-3^{m-1}}[c,a]\in Z(G),\quad (a^{-3^{m-1}}[c,a])^{3^{m+u}}=1.$$

于是对某个 j, $a^{-3^{m-1}}[c,a]=c^{j3^{v-1}}$. 由此可得, $[c,a]=a^{3^{m-1}}c^{j3^{v-1}}$. 注意到 $[c,a]^3=1$ 且 $a^{3^m}=c^{3^v}$. 有 $j+1\equiv 0(\bmod 3^{m+u-1})$, 即对某个 k, $j=-1+k3^{m+u-1}$. 因而

$$[c,a]=a^{3^{m-1}}c^{-(1-k3^{m+u-1})3^{v-1}}.$$

用 $c^{1-k3^{m+u-1}}$ 替换 c 可得

$$e=[c,a]=a^{3^{m-1}}c^{-3^{v-1}}.$$

由此可得, $c^{3^{v-1}}\in\langle a,b,e\rangle$. 断言 $c^{3^{v-2}}\notin\langle a,b,e\rangle$. 若 $v=2$, 则 $c=c^{3^{v-2}}\notin\langle a,b,e\rangle$. 若 $v>2$, 设 $c^{3^{v-2}}\in\langle a,b,e\rangle$. 因为 $c^3\in Z(G)$, 有 $c^{3^{v-2}}\in Z(\langle a,b,e\rangle)=\langle a^{-3^{m-1}}e\rangle$. 因而

$$o(c^{3^{v-2}})\leqslant 3^{m+u},\quad o(c)\leqslant 3^{m+u+v-2}.$$

矛盾. 因为 $c\in N_G(\langle a,b,e\rangle)$, 所以 $G=(\langle a,b\rangle\rtimes\langle e\rangle)\langle c\rangle$. 我们得到群 (II). 因为 $|G|=3^{3m+u+v}$, $\exp(G)=3^{2m+u-1}$, 所以不同的参数 u,v 对应的群不同构.

情形 2 $\langle d^3\rangle>\langle a^{3^m}\rangle$.

令 $a^{3^m}=d^{l3^u}$, 其中 $3\nmid l$, $1<u\leqslant m$. 则 $o(a)=3^{2m-u}$. 分别用 b 和 d 的适当幂替换 b 和 d, 有 $a^{3^m}=d^{3^u}$, 且仍然有

$$b^{3^m}=d^{3^m}=1,\quad [a,b]=d,\quad [b,c]=b^{-3^{m-1}},\quad [a,b,c]=[b,c,a]=[c,a,b]=d^{3^{m-1}}.$$

通过简单的计算可得

$$a^{-3^{m-1}}[c,a]\in Z(G),\quad (a^{-3^{m-1}}[c,a])^{3^{m-u+1}}=1.$$

于是对某个整数 i, 有 $a^{-3^{m-1}}[c,a]=d^{i3^{u-1}}$. 从而 $[c,a]=a^{3^{m-1}}d^{i3^{u-1}}$. 注意到 $[c,a]^3=1$ 且 $a^{3^m}=d^{3^u}$. 我们有 $i+1\equiv 0(\mathrm{mod}\ 3^{m-u})$, 即对某个整数 k, $i=-1+k3^{m-u}$. 因而

$$[c,a]=a^{3^{m-1}}d^{-3^{u-1}}d^{k3^{m-1}}.$$

再用 $cb^{k3^{m-1}}$ 替换 c 可得, $[c,a]=a^{3^{m-1}}d^{-3^{u-1}}$.

明显地, $a^{3^{m-1}}\notin\langle d\rangle$. 注意到 $a^{3^m}=d^{3^u}$ 且 $[d,a]=1$. 于是 $\langle a,d\rangle\cong \mathrm{C}_{3^{2m-u}}\times \mathrm{C}_{3^u}$. 又因为 $[b^{3^{m-1}},a]\neq 1$, 故 $b^{3^{m-1}}\notin\langle a,d\rangle$. 注意到 $b\in N_G(\langle a,d\rangle)$ 且 $o(b)=3^m$. 我们有

$$\langle a,b\rangle=\langle a,d\rangle\rtimes\langle b\rangle,\quad |\langle a,b\rangle|=3^{3m}.$$

(i) 若 $c^3=1$, 则

$$G=\langle a,b\rangle\rtimes\langle c\rangle,\quad |G|=3^{3m+1},\quad \exp(G)=3^{2m-u}.$$

此时 G 是群 (III), 且不同的参数 u 给出的群不同构.

(ii) 若 $o(c)>3^m$, 因为 $\langle d^3\rangle<\langle c^3\rangle$, 我们有 $d^3=c^{i3^v}$, 其中 $3\nmid i$, $v>1$. 于是 $o(c)=3^{m+v-1}$. 分别用 a 和 d 的适当幂替换 a 和 d, 有 $d^3=c^{3^v}$. 断言 $c^{3^{v-1}}\notin\langle a,b\rangle$.

若否, 因为 $c^3 \in Z(G)$, 故 $c^{3^{v-1}} \in \langle d^3 \rangle$. 从而 $o(c^{3^{v-1}}) \leqslant 3^{m-1}$ 且 $o(c) \leqslant 3^{m+v-2}$, 矛盾. 因为 $c \in N_G(\langle a, b \rangle)$, 有

$$G = \langle a, b \rangle \langle c \rangle, \quad |G| = 3^{3m+v}, \quad \exp(G) = \max\{o(a), o(c)\}.$$

若 $o(a) > o(c)$, 则 $3^{2m-u} > 3^{m+v-1} \geqslant 3^{m+1}$. 因而 $v < m - u + 1$ 且 $u < m - 1$. 此时 G 为群 (Ⅳ), 显然, 不同的参数 u, v 给出的群不同构.

若 $o(a) \leqslant o(c)$, 由于 $a^{3^m}, c^3 \in Z(G)$, 则 $a^{3^m} \in \langle c^{3^m} \rangle$. 不妨设 $a^{3^m} = c^{i3^m}$. 用 ac^{-i} 替换 a, 即得 $a^{3^m} = 1$. 从而 $[c, a] = a^{3^{m-1}} d^{-3^{m-1}}$. 用 $c[b, c]$ 替换 c 可得 $[c, a] = a^{3^{m-1}}$. 此时 G 为群 (Ⅴ). 显然, 不同的参数 v 给出的群不同构. □

综上所证, 有限 p 群 G 是极小非 $\mathcal{P}_2$ 群当且仅当 G 或是 p^4 阶的极大类群或是定理 13.2.6—定理 13.2.10 中所列的群之一.

13.3　内 $\mathcal{P}_n$-p 群的某些性质

有限群 G 称为一个**内 $\mathcal{P}_n$ 群**, 如果 G 的幂零类大于 n, 但是 G 的所有真子群的幂零类都不超过 n. 显然, 内 $\mathcal{P}_1$ 群就是内交换群. 若 $n \geqslant 2$, 则非幂零的内 $\mathcal{P}_n$ 群就是内幂零群. 而幂零的内 $\mathcal{P}_n$ 群一定是 p 群. 所以内 $\mathcal{P}_2$-p 群的分类可以看作是内交换 p 群分类的一个自然的、较大的推广.

由于类 2 的 p 群在有限 p 群中的重要性, Berkovich 在其 p 群专著 [26] 中提出了如下问题.

Problem 87(old problem)　Study the p-groups of class 3 all of whose proper subgroups are of class $\leqslant 2$.

显然, Problem 87 就是研究内 $\mathcal{P}_2$-p 群. 文献 [144] 证明了: 若 G 是内 $\mathcal{P}_2$-p 群, 则 $c(G) = 3$. 文献 [127] 给出了这个结果的一个简短证明. 这意味着 Problem 87 中的条件 “class 3” 可以去掉.

文献 [127] 研究了内 $\mathcal{P}_n$ 群的一般性质, 进一步地, 对于 $p > 3$, 文献 [125],[126] 分类了内 $\mathcal{P}_2$ 群. 对于 $p = 2, 3$, 内 $\mathcal{P}_2$ 群的分类有待解决. 本节介绍内 $\mathcal{P}_n$-p 群的一般性质, 13.4 节将介绍其分类.

定理 13.3.1　*设 G 是内 $\mathcal{P}_n$- p 群. 则*

(1) 若 $n = 2$, 则 $d(G) \leqslant 3$;

(2) 若 $n > 2$, 则 $d(G) \leqslant n$.

证明　(1) 设 $d(G) \geqslant 4$. 对于 $a, b, c \in G$, 令 $H = \langle a, b, c \rangle$. 则 $H < G$. 因为 G 是内 $\mathcal{P}_2$-p 群, 故 $[a, b, c] = 1$. 于是 $c(G) \leqslant 2$. 矛盾.

(2) 设 $d(G) \geqslant n + 1$. 取 $H \leqslant G$ 使得 $d(H) = n$. 则 $H < G$. 因为 G 是内 $\mathcal{P}_n$-p 群, 故 $c(H) \leqslant n$. 由 [89] 中的Ⅲ, 定理 6.10 可得 $c(G) \leqslant n$. 矛盾. □

下列例子表明, 存在内 $\mathcal{P}_2$-p 群使得 $d(G)=3$.

例 13.3.2 设 $G=\langle a,b,c,d,e,f,x \mid a^3=b^3=c^3=d^3=e^3=f^3=x^3=1,[b,a]=d,[c,a]=e,[c,b]=f,[d,c]=x,[e,b]=x^2,[f,a]=x,[d,a]=[d,b]=[e,a]=[e,c]=[f,b]=[f,c]=[x,a]=[x,b]=[x,c]=1\rangle$. 则 G 是内 $\mathcal{P}_2$-p 群且 $d(G)=3$.

证明 首先断言: $|G|=3^7$. 由命题 1.1.5(1) 可得 $G_3=\langle x\rangle$. 再由 [89] 中的III, 引理 2.11 b 可得, $\langle d,e,f,x\rangle$ 是交换的. 令

$$H=\langle a,c,d,e,f,x\rangle,\quad H_1=\langle f,a,x\rangle,\quad H_2=\langle c,d,x\rangle.$$

则

$$H_1\cong H_2\cong \mathrm{M}_3(1,1,1),\quad H=H_1*H_2\times\langle e\rangle.$$

于是 $|H|=3^6$. 现在有 $G=\langle H,b\rangle$, $H\lhd G$, $b\notin H$ 且 $b^3\in H$. 这意味着 $|G/H|=3$ 且 $|G|=3^7$.

其次断言: $d(G)=3$. 事实上, $G=\langle a,b,c\rangle$. 于是 $G'=\langle d,e,f,x\rangle\cong \mathrm{C}_3^4$. 由命题 1.1.10 可知, $\mho_1(G)\leqslant G'$. 于是 $\Phi(G)=G'$. 从而 $d(G)=3$.

最后断言: G 是内 $\mathcal{P}_2$-p 群. 只需证 G 的极大子群的幂零类不超过 2 即可. 因为 $G=\langle a,b,c\rangle$ 且 $d(G)=3$, 故 G 的极大子群只能是如下子群:

$$\langle b,c,\Phi(G)\rangle,\quad \langle ab^i,c,\Phi(G)\rangle,\quad \langle ac^i,bc^j,\Phi(G)\rangle,\quad 其中\ 1\leqslant i,j\leqslant 3.$$

因为 $G_4=1$ 且 $G'=\Phi(G)$, 只需证

$$[c,b,b]=[c,b,c]=[c,ab^i,ab^i]=[c,ab^i,c]=[ac^i,bc^j,bc^j]=[ac^i,bc^j,ac^i]=1.$$

明显地, $[c,b,b]=[c,b,c]=1$. 通过简单的计算可知, 其他的等式也成立. □

引理 13.3.3 设 G 是有限 p 群. 若 $d(G)=2$ 且 $G_5=1$, 则 G 亚交换.

证明 令 $G=\langle a,b\rangle$. 则 $G'=\langle [a,b],G_3\rangle$. 因为

$$[[a,b],G_3]\leqslant [G_2,G_3]\leqslant G_5=1,\quad [G_3,G_3]\leqslant G_5=1,$$

故 $G''=1$. □

定理 13.3.4 设 G 内 $\mathcal{P}_2$-p 群. 则 $c(G)=3$.

证明 设 G 是极小阶反例. 则 $|G_4|=p$. 取 $x_1,x_2,x_3,x_4\in G$ 使得

$$[x_1,x_2,x_3,x_4]\neq 1.$$

因为 $\langle [x_1,x_2],x_3,x_4\rangle$ 的幂零类大于 2, 故

$$\langle [x_1,x_2],x_3,x_4\rangle=G.$$

由 $[x_1, x_2] \in G' \subseteq \Phi(G)$ 可知, $d(G) = 2$. 令 $G = \langle a, b \rangle$ 且 $c = [a, b]$. 则

$$G_4 = \langle [c, a, a], [c, b, b], [c, b, a], [c, a, b] \rangle.$$

因为 $d(G) = 2$ 及 G 是内 $\mathcal{P}_2$-p 群, 故对于 $x \in \Phi(G)$, $y \in G$, 有 $[x, y, y] = 1$. 从而 $[c, a, a] = [c, b, b] = 1$. 由引理 13.3.3 可知, G 亚交换. 又由命题 1.1.8(5) 可得, $[c, a, b] = [c, b, a]$. 于是 $G_4 = \langle [c, a, b] \rangle$. 因为

$$[c, a, b]^2 = [c, a, b][c, b, a] = [c, a, a][c, a, b][c, b, a][c, b, b] = [c, ab, ab] = 1,$$

故 $p = 2$. 又因为 $a^2, b^2 \in \Phi(G)$, 有 $[a^2, b, b] = 1$ 且 $[b^2, ba, ba] = 1$. 另一方面,

$$\begin{aligned}[b^2, ba, ba] &= [b^2, a, ba] = [b^2, a, a][b^2, a, b][b^2, a, b, a] = [b^2, a, b] = [[b, a]^2[b, a, b], b] \\ &= [[b, a]^2, b] = [b, a, b]^2 = [a, b, b]^{-2} = [c, b]^{-2}.\end{aligned}$$

故有 $[c, b]^{-2} = 1$. 于是

$$[c, a, b] = [c, b]^2[c, a, b] = [c^2, b][c, a, b] = [c^2[c, a], b] = [a^2, b, b] = 1.$$

这意味着 $G_4 = 1$. 与 $|G_4| = p$ 矛盾. □

下列例子表明, 存在内 $\mathcal{P}_3$-p 群使得 $c(G) \neq 4$.

例 13.3.5　设 $G = \langle a, b, c, d, e, f, g, h, x \mid a^5 = b^5 = c^5 = d^5 = e^5 = f^5 = g^5 = h^5 = x^5 = 1, [b, a] = c, [c, a] = d, [c, b] = e, [d, a] = f, [d, b] = g, [e, a] = g, [e, b] = h, [f, a] = 1, [f, b] = x, [g, a] = x^2, [g, b] = x^2, [h, a] = x, [h, b] = 1, [x, a] = [x, b] = 1 \rangle$. 则 G 是内 $\mathcal{P}_3$-p 群且 $c(G) = 5$.

证明　首先, $G = \langle a, b \rangle$. 由命题 1.1.5(1) 可得 $G_5 = \langle x \rangle$. 于是 $c(G) = 5$.

断言: $|G| = 5^9$. 令

$$K = \langle d, e, f, g, h, x \rangle, \quad H = \langle c, K \rangle, \quad M = \langle a, H \rangle.$$

因为 $G_6 = 1$, 故 $K \cong C_5^6$. 由于 $K \lhd H, c \notin K$ 且 $c^3 \in K$, 有 $|H| = 5^7$. 又由 $H \lhd M, a \notin H$ 且 $a^3 \in H$ 可得 $|M| = 5^8$. 明显地, $G = \langle b, M \rangle$. 由 $M \lhd G, b \notin M$ 且 $b^3 \in M$ 可得 $|G| = 5^9$.

下证 G 是内 $\mathcal{P}_3$-p 群. 只需证 G 的极大子群的幂零类不超过 3 即可. G 的极大子群只能是: $\langle b, \Phi(G) \rangle$ 或 $\langle ab^i, \Phi(G) \rangle$, 其中 $1 \leqslant i \leqslant p$. 因为 $K \leqslant G'$, $|G/K| = 5^2$ 且 $d(G) = 2$, 故 $G' = \Phi(G)$. 又 $G_6 = 1$ 且 $G' = \Phi(G)$, 只需证 $[c, b, b, b] = 1$ 且 $[c, ab^i, ab^i, ab^i] = 1$ 即可. 明显地, $[c, b, b, b] = 1$. 通过计算也有 $[c, ab^i, ab^i, ab^i] = 1$. 结论得证. □

在例 13.3.5 中, 容易验证, G/G_5 是内 $\mathcal{P}_3$-p 群, 且 $c(G/G_5) = 4$.

引理 13.3.6 设 G 是群, $H \trianglelefteq G$. 令 $T = \{g_1, g_2, \cdots, g_n\} \subseteq G$, 其中 T 中仅有 m 个元素属于 H, $n \geqslant 2$, $m \geqslant 1$. 则 $[g_1, g_2, \cdots, g_n] \in H_m$.

证明 对 n 作归纳. 若 $n = 2$, 则 $m = 1$ 或 2. 若 $m = 1$, 由 $H \trianglelefteq G$ 可得 $[g_1, g_2] \in H = H_1$. 若 $m = 2$, 明显地, $[g_1, g_2] \in H_2$. 因而对于 $n = 2$ 结论成立. 假设结论对于 $n = k$ 成立. 若 $n = k + 1$, 分两种情形讨论. 若 $g_n \notin H$, 由归纳假设可得, $[g_1, \cdots, g_k] \in H_m$. 因为 $H_m \trianglelefteq G$, 故 $[g_1, \cdots, g_k, g_{k+1}] \in H_m$. 若 $g_n \in H$, 对于 $m = 1$, 结论明显成立. 设 $m \geqslant 2$. 由归纳假设可得, $[g_1, \cdots, g_k] \in H_{m-1}$. 于是 $[g_1, \cdots, g_k, g_{k+1}] \in H_m$. □

定理 13.3.7 设 G 是内 $\mathcal{P}_n$-p 群, $d(G) = d$. 则 $c(G) \leqslant \dfrac{dn}{d-1}$.

证明 设 $G = \langle a_1, a_2, \cdots, a_d \rangle$ 且 $y = \left[\dfrac{dn}{d-1}\right]$. 令 $g_1, g_2, \cdots, g_{y+1}$ 是任意一个长为 $y + 1$ 的序列, 其中该序列中的每个元素取自 G 的生成集 $\{a_1, a_2, \cdots, a_d\}$. 下证

$$[g_1, g_2, \cdots, g_{y+1}] = 1.$$

对每个 $i \in \{1, \cdots, d\}$, 令 n_i 表示 a_i 出现在这个序列中的次数. 于是

$$n_1 + n_2 + \cdots + n_d = y + 1.$$

对于 $i > j$, 不妨设 $n_i \geqslant n_j$. 令

$$M = \langle \Phi(G), a_1, a_2, \cdots, a_{d-1} \rangle.$$

注意到 M 是 G 的极大子群. 由引理 13.3.6 可得

$$[g_1, g_2, \cdots, g_{y+1}] \in M_r, \quad \text{其中 } r = y + 1 - n_d.$$

因为 $n_d \leqslant \dfrac{y+1}{d}$, 故 $r \geqslant y + 1 - \dfrac{y+1}{d} > n$. 又因为 G 是内 $\mathcal{P}_n$-p 群, 故 $M_r = 1$. 由此可得

$$[g_1, g_2, \cdots, g_{y+1}] = 1.$$

由命题 1.1.5(1) 可得, $c(G) \leqslant y$. 明显地, $y \leqslant \dfrac{dn}{d-1}$. 从而 $c(G) \leqslant \dfrac{dn}{d-1}$. □

定理 13.3.8 设 G 是有限 p 群且 $p \neq 3$. 对于每个 $g, h \in G$, 若 $[g, h, h] = 1$, 则 $c(G) \leqslant 2$.

证明 设 G 是极小阶反例. 则 G 是内 $\mathcal{P}_2$-p 群. 由定理 13.3.4 可得, 存在 $a, b, c \in H$ 使得 $[a, b, c] \neq 1$. 因为 G 亚交换, 故

$$[a, b, c][b, c, a][c, a, b] = 1.$$

又因为 $G_4=1$, 故

$$[b,ca,ca]=[b,c,a][b,c,c][b,a,c][b,a,a]=[b,c,a][b,a,c]=[b,c,a][a,b,c]^{-1}.$$

又 $[b,ca,ca]=1$, 故 $[a,b,c]=[b,c,a]$. 类似可证, $[b,c,a]=[c,a,b]$. 于是 $[a,b,c]^3=1$. 矛盾于 $p\neq 3$. □

定理 13.3.9　G 是内 $\mathcal{P}_2$-p 群. 则

(1) G' 是交换群.

(2) $\exp(G_3)=p$.

(3) $[\Phi(G),G]\leqslant Z(G)$.

(4) $\mho_1(G')\leqslant Z(G)$.

(5) $Z(G)\leqslant \Phi(G)$.

(6) 若 $d(G)=3$, 则 $p=3$ 且 G 正则. 令 $G=\langle a,b,c\rangle$. 则 $[a,b,c]=[b,c,a]=[c,a,b]\neq 1$.

(7) 若 $p>3$, 则 G 正则.

证明　(1) 由定理 13.3.4 可得 $c(G)=3$. 于是 $G_4=1$. 由此可得 $[G',G']=[G_2,G_2]\leqslant G_4=1$. 从而 G' 交换.

(2) 由定理 13.3.4 可得 $G_4=1$. 又由定理 13.3.1 可得 $d(G)\leqslant 3$. 若 $d(G)=3$, 则对于 $a,b,c\in G$, $\langle a^p,b,c\rangle<G$. 于是 $c(\langle a^p,b,c\rangle)\leqslant 2$. 由此可得 $[a^p,b,c]=1$. 由命题 13.2.1 可得, $[a,b,c]^p=[a^p,b,c]$. 从而 $[a,b,c]^p=1$. 也即 $\exp(G_3)=p$. 若 $d(G)=2$, 设 $G=\langle a,b\rangle$. 则 $G_3=\langle [a,b,b],[a,b,a]\rangle$. 因为 $\langle a,b^p\rangle<G$, 故 $c(\langle a,b^p\rangle)\leqslant 2$. 从而 $[a,b^p,a]=1$. 再由命题 13.2.1 可得, $[a,b,a]^p=[a,b^p,a]$. 于是 $[a,b,a]^p=1$. 类似可证, $[a,b,b]^p=1$. 也即 $\exp(G_3)=p$.

与命题 13.2.2(2)—(5) 的证明方法相同可得 (3)—(6). 由定理 1.11.4(1) 可得 (7). □

定理 13.3.10　设 G 是有限 p 群. 则

(1) G 是二元生成的内 $\mathcal{P}_2$ 群当且仅当 $\exp(G_3)=p$ 且 $c(G)=3$;

(2) G 是三元生成的内 $\mathcal{P}_2$ 群当且仅当 $\exp(G_3)=p$ 且对于任意的 $a,b\in G$ 均有 $[a,b,b]=1$.

证明　(1) $\Longrightarrow$: 由定理 13.3.4 和定理 13.3.9(2) 直接得到.

$\Longleftarrow$: 只需证 G 的每个极大子群的幂零类不超过 2 即可. 令 H 是 G 的极大子群. 则存在 $a\in H\backslash\Phi(G)$ 和 $b\in G\backslash H$ 使得 $G=\langle a,b\rangle$. 显然, $H=\langle a,\Phi(G)\rangle$. 因为 $\Phi(G)=G'\mho_1(G)$, 故

$$H_3=\langle [x,y,z]\mid x,y,z\in\{a\}\cup G'\cup\mho_1(G)\rangle.$$

若 $\{x,y,z\}$ 中有一个元素属于 $\mho_1(G)$, 由命题 13.2.1 及 $\exp(G_3)=p$ 可得, $[x,y,z]=1$. 若 $\{x,y,z\}$ 中有一个元素属于 G', 由于 $c(G)=3$, 我们也有 $[x,y,z]=1$. 因而 $H_3=1$.

(2) $\Longrightarrow$: 因为 $d(G)=3$, 故对于 $a,b\in G$, $\langle a,b\rangle<G$. 因为 G 是内 $\mathcal{P}_2$ 群, 故 $[a,b,b]=1$. 另一方面, 由定理 13.3.9(2) 可得 $\exp(G_3)=p$.

$\Longleftarrow$: 与 (1) 的证明方法相同, 可得结论. □

定理 13.3.11 *设 G 是内 $\mathcal{P}_2$ 群且 $\overline{G}=G/G_3$. 则*

(1) $c(\overline{G})=2$, $d(\overline{G})=d(G)$.

(2) 若 $d(\overline{G})=2$, 则 $G_3\cong \mathrm{C}_p$ 或 C_p^2; 若 $d(\overline{G})=3$, 则 $G_3\cong \mathrm{C}_p$.

(3) 若 $d(\overline{G})=3$, 则 $p=3$ 且 $d(\overline{G}')=3$.

证明 (1) 明显地, $c(\overline{G})=2$. 因为 $G_3\leqslant\Phi(G)$, 故 $\Phi(\overline{G})=\Phi(G)/G_3$. 于是 $d(G)=d(\overline{G})$.

(2) 若 $d(\overline{G})=2$, 由 (1) 可得 $d(G)=2$. 令 $G=\langle a,b\rangle$. 则 $G_3=\langle [a,b,a],[a,b,b]\rangle$. 由定理 13.3.9(2) 可得, $G_3\cong \mathrm{C}_p$ 或 C_p^2.

若 $d(\overline{G})=3$, 则 $d(G)=3$. 于是对于 $a,b\in G$, $\langle a,b\rangle<G$. 因为 G 是内 $\mathcal{P}_2$ 群, 故 $[a,b,b]=1$. 令 $G=\langle a,b,c\rangle$. 则

$$G_3=\langle [a,b,c],[a,c,b],[b,c,a]\rangle.$$

因为 $[a,c,b]=[c,a,b]^{-1}$, 由定理 13.3.9(6) 可得 $G_3\cong \mathrm{C}_p$.

(3) 由 (1) 可得 $d(G)\leqslant 3$. 于是对于 $a,b\in G$, $[a,b,b]=1$. 若 $p\neq 3$, 由定理 13.3.8 可得 $c(G)\leqslant 2$. 这矛盾于定理 13.3.4. 故 $p=3$.

令 $G=\langle a,b,c\rangle$. 则 $\overline{G}=\langle [\bar a,\bar b],[\bar a,\bar c],[\bar b,\bar c]\rangle$. 若 $d(\overline{G}')\neq 3$, 不妨设 $[\bar a,\bar b]=[\bar a,\bar c]^s[\bar b,\bar c]^t$. 则

$$[a,b,c]=[a,c^s,c][b,c^t,c]=1.$$

这矛盾于定理 13.3.9(6). □

由定理 13.3.11 我们观察到, 若 G 是内 $\mathcal{P}_2$ 群, 则 G 分别是 G_3 被幂零类为 2 的生成元为 2 或 3 的群 H 的中心扩张. 事实上, 定理 13.3.11 给出了分类内 $\mathcal{P}_2$ 群的框架及一般方法.

13.4 内 $\mathcal{P}_2$-p 群的分类

由定理 13.3.11 我们观察到, 若 G 是内 $\mathcal{P}_2$ 群, 则 G 分别是 G_3 被幂零类为 2 的生成元为 2 或 3 的群 H 的中心扩张. 特别是, 若 $d(H)=3$, 则 $p=3$. 若 $p>3$, 则内 $\mathcal{P}_2$ 群 G 就是 G_3 被 H 的扩张, 其中 $d(H)=2$ 且 $c(H)=2$. 本节分类内 $\mathcal{P}_2$-p 群, 其中 $p>3$.

首先我们给出二元生成幂零类为 2 的有限 p 群的分类. 对 $p>2$, 文献 [13] 给出了分类. 而对于 $p=2$, 文献 [108] 给出了分类. 文献 [125] 对 $p>2$ 的情形又独立地给出了同构分类. 这里我们采用文献 [125] 的证明.

定理 13.4.1　设 G 是奇数阶亚循环 p 群. 则 G 满足 $d(G)=2$ 且 $c(G)=2$ 当且仅当 G 与下列群同构.

$$G=\langle a,b \mid a^{p^{r+s+u}}=1, b^{p^{r+s+t}}=a^{p^{r+s}}, [a,b]=a^{p^r}\rangle,$$

其中 r,s,t,u 是非负整数满足 $r\geqslant 1$ 且 $s+u\leqslant r$. 参数 r,s,t 和 u 的不同值给出不同构的群.

证明　由定理 6.1.3 及 $c(G)=2$ 易得 $s+u\leqslant r$. 反之, 通过简单的验证可知, 定理中的群是幂零类为 2 的. □

定理 13.4.2　设 G 是非亚循环群, m,n,r,s,t 是正整数. 则 G 满足 $d(G)=2$ 且 $c(G)=2$ 当且仅当 G 同构于下列互不同构的群之一.

(A1) $\langle a,b,c \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=1, [c,a]=[c,b]=1\rangle$, $m\geqslant n\geqslant r$;

(A2) $\langle a,b,c \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=[c,b]=1\rangle$, $m\geqslant n>r$, $n>t\geqslant (n+r)/2$;

(A3) $\langle a,b,c \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=[c,b]=1\rangle$, $m>n>r$, $m>s\geqslant (m+r)/2$, $n\geqslant m+r-s$;

(A4) $\langle a,b,c \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=[c,b]=1\rangle$, $m>n>r$, $m>s>t>r, s+n<m+t, n>t\geqslant m-s+r$.

定理中所有的群均有阶 p^{m+n+r}.

证明　因为 $d(G)=2$ 且 $c(G)=2$, 故 G' 循环. 于是

$$|G/\mho_1(G)|=|G/\Phi(G)||\Phi(G)/\mho_1(G)|=|G/\Phi(G)||G'\mho_1(G)/\mho_1(G)|\leqslant p^3.$$

由此可得 $\omega(G)\leqslant 3$. 若 $\omega(G)\leqslant 2$, 由定理 7.2.1 可得 G 亚循环. 与假设矛盾. 故 $\omega(G)=3$.

令 $a\in G\backslash\Phi(G)$ 使得 a 有极大阶, $b\in G\backslash\langle a,\Phi(G)\rangle$ 使得 b 有极小阶. 因为 $d(G)=2$, 可设 $G=\langle a,b\rangle$. 令

$$o(a)=p^m,\quad o(b)=p^n,\quad [a,b]=c.$$

断言 $\langle a\rangle\bigcap\langle b\rangle=1$. 若否, 不妨设 $b^{p^{n-1}}=a^{i_1p^{m-1}}$. 则存在 $b'=ba^{-i_1p^{m-n}}c^{k_1}\in G\backslash\langle a,\Phi(G)\rangle$ 使得 $o(b')=p^{n-1}<o(b)$. 矛盾. 令 r_1 是使得 c^{r_1} 可表为形如 $a^{s_1}b^{t_1}$ 的最小正整数. 不妨设 s 满足 $p^s\mid s_1$ 但 $p^{s+1}\nmid s_1$, t 满足 $p^t\mid t_1$ 但 $p^{t+1}\nmid t_1$, $r_1=i_1p^r$, 其中 $(i_1,p)=1$.

断言 $r_1 = p^r$. 因为 $(i_1, p) = 1$, 故 $(i_1, o(c)) = 1$. 于是存在 j_1 使得 $i_1 j_1 \equiv 1(\mathrm{mod}\ o(c))$. 因为 $c(G) = 2$, 故 $a^{s_1}, b^{t_1} \in Z(G)$. 由此可得

$$c^{p^r} = (c^{i_1 p^r})^{j_1} = (c^{r_1})^{j_1} = (a^{s_1} b^{t_1})^{j_1} = a^{j_1 s_1} b^{j_1 t_1}.$$

于是 $p^r \geqslant r_1 = i_1 p^r$, 即 $r_1 = p^r$.

因为 $c(G) = 2$, 故 $c^{p^n} = [a, b^{p^n}] = 1$. 由此可得 $n \geqslant r$. 因为 $\omega(G) = 3$, 故 $r \geqslant 1$. 不妨设 $G = \langle a, b, c \mid a^{p^m} = 1, b^{p^n} = 1, [a,b] = c, c^{p^r} = a^{ip^s} b^{jp^t}, [c,a] = [c,b] = 1\rangle$, 其中 $m \geqslant n \geqslant r \geqslant 1$.

若 $c^{p^r} = 1$, 则我们得到群 (A1). 设 $c^{p^r} \neq 1$. 分三种情形讨论.

情形 1 $a^{ip^s} = 1$.

在这种情形下,

$$G = \langle a, b, c \mid a^{p^m} = 1, b^{p^n} = 1, [a,b] = c, c^{p^r} = b^{jp^t}, [c,a] = [c,b] = 1\rangle.$$

因为 $c^{p^r} \neq 1$, 故 $j \not\equiv 0(\mathrm{mod}\ p)$. 于是存在 x 使得 $xj \equiv 1(\mathrm{mod}\ p)$. 用 a 替换 a^x, c 替换 c^x 可得

$$G = \langle a, b, c \mid a^{p^m} = 1, b^{p^n} = 1, [a,b] = c, c^{p^r} = b^{p^t}, [c,a] = [c,b] = 1\rangle.$$

因为 $b^{jp^t} \neq 1$, 故 $t < n$. 又 $c^{p^r} = b^{p^t}$, 故 $o(c) = p^{n-t+r}$. 另一方面,

$$c^{p^t} = [a, b^{p^t}] = [a, c^{p^r}] = 1.$$

故 $t \geqslant n - t + r$, 即 $t \geqslant (n+r)/2$. 因为 $c^{p^n} = [a, b^{p^n}] = 1$, 故 $n \geqslant n - t + r$, 即 $t \geqslant r$. 由此可得 $n > r$. 现在我们有

$$m \geqslant n > r \geqslant 1, \quad n > t \geqslant (n+r)/2.$$

我们得到群 (A2).

情形 2 $b^{jp^t} = 1$.

在这种情形下,

$$G = \langle a, b, c \mid a^{p^m} = 1, b^{p^n} = 1, [a,b] = c, c^{p^r} = a^{ip^s}, [c,a] = [c,b] = 1\rangle.$$

因为 $(i, p) = 1$, 存在 x 使得 $xi \equiv 1(\mathrm{mod}\ p)$. 用 b 替换 b^x, c 替换 c^x 可得

$$G = \langle a, b, c \mid a^{p^m} = 1, b^{p^n} = 1, [a,b] = c, c^{p^r} = a^{p^s}, [c,a] = [c,b] = 1\rangle.$$

若 $m = n$, 用 a 替换 b^{-1}, b 替换 a, 这归结到情形 1. 设 $m > n$. 因为 $a^{ip^s} \neq 1$, 故 $s < m$. 又 $c^{p^r} = a^{p^s}$, 故 $o(c) = p^{m-s+r}$. 另一方面,

$$c^{p^s} = [a^{p^s}, b] = [c^{p^r}, b] = 1.$$

于是 $s \geqslant m-s+r$. 也即 $s \geqslant (m+r)/2$. 因为 $c^{p^n}=[a,b^{p^n}]=1$, 故 $n \geqslant m-s+r$. 由此可得 $n>r$. 现在有

$$m>n>r\geqslant 1,\quad m>s\geqslant (m+r)/2,\quad n\geqslant m+r-s.$$

得到群 (A3).

情形 3　$a^{ip^s}\neq 1$ 且 $b^{jp^t}\neq 1$.

在这种情形下,

$$G=\langle a,b,c \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{ip^s}b^{jp^t}, [c,a]=[c,b]=1\rangle.$$

此时存在 x 和 y 使得 $xi\equiv 1(\bmod p)$ 且 $yj\equiv 1(\bmod p)$. 用 a 替换 a^y, b 替换 b^x, c 替换 c^{xy} 可得

$$G=\langle a,b,c \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=[c,b]=1\rangle.$$

因为 $a^{ip^s}\neq 1$, 故 $s<m$. 又 $b^{jp^t}\neq 1$, 故 $t<n$. 另一方面,

$$c^{p^s}=[a^{p^s},b]=[c^{p^r}b^{-p^t},b]=1.$$

故 $p^s\geqslant o(c)$. 由此可得 G 是 p^s 交换的. 同理可得, $p^t\geqslant o(c)$, 从而 G 是 p^t 交换的. 因为 $c^{p^n}=[a,b^{p^n}]=1$, 故 $p^n\geqslant o(c)$.

若 $s\leqslant t$, 用 a 替换 $b^{p^{t-s}}a$ 可得

$$G=\langle a,b,c \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=[c,b]=1\rangle.$$

这归结为情形 2.

设 $s>t$. 若 $n-t\geqslant m-s$, 用 b 替换 $a^{p^{s-t}}b$ 可得

$$G=\langle a,b,c \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=[c,b]=1\rangle.$$

这归结为情形 1. 不妨设 $n-t<m-s$. 因为 $c^{p^r}=a^{p^s}b^{p^t}$ 且 $n-t<m-s$, 故 $o(c)=p^{m-s+r}$. 又 $p^t\geqslant o(c)$, 故 $t\geqslant m-s+r$. 因为 $s>t$ 且 $n>t$, 故 $p^s\geqslant o(c)$ 且 $p^n\geqslant o(c)$. 又 $t\geqslant m-s+r$ 且 $m>s$, 故 $t>r$. 因为 $s>t$ 且 $s-t<m-n$, 故 $m>n$. 现在有

$$m>n>r\geqslant 1,\quad m>s>t>r,\quad s+n<m+t,\quad n>t\geqslant m-s+r.$$

得到群 (A4).

我们可证: $|G|=p^{m+n+r}$. 设 G 是群 (A4), $H=\langle b,c\rangle<G$. 则

$$H\cong \mathrm{C}_{p^n}\times \mathrm{C}_{p^{m-s+r}}.$$

令 $\sigma(g): h \longrightarrow h^g$, 其中 $h \in H$, $g \in G$. 则

$$\sigma(a) \in \mathrm{Aut}(H), \quad \sigma^{p^m}(a) = \sigma(c^{p^r} b^{-p^t}).$$

明显地, $a^{p^s} = c^{p^r} b^{-p^t} \in H$. 因为

$$a^{p^{s-1}} \notin H, \quad (c^{p^r} b^{-p^t})^a = c^{p^r} b^{-p^t},$$

故 G 是 H 被 C_{p^s} 的扩张. 于是 $|G| = p^{m+n+r}$. 类似地, 定理中其他群的阶也为 p^{m+n+r}.

现在以群 (A4) 为例证明定理中的群满足假设条件. 因为 $G = \langle a, b\rangle$ 且 G 不循环, 故 $d(G) = 2$. 明显地, $c(G) = 2$. 因为 $c(G) < p$, 由定理 1.11.4(1) 可知, G 正则. 令 $d = ca^{-p^{s-r}} b^{-p^{t-r}}$. 由命题 1.1.9 和命题 1.1.10 可得, $o(d) = p^r$. 不难证明, (a, b, d) 是 G 的一组唯一性基. 由 [77] 中的定理 4.51 可知, G 的型是 (m, n, r). 于是 $\omega(G) = 3$. 由定理 7.2.1 可知, G 非亚循环. 故 G 满足所有假设条件.

最后证明定理中的群互不同构. 注意到, 对于群 (A1)—(A4), (m, n, r) 是不变量且定理中的群有如表 13.1 所示的信息. 对于群 (A4), G 是 p^t 交换的. 由 [89] 中的III, 引理 10.5 可知, $\mho_t(G) \cong \mathrm{C}_{p^{m-t}} \times \mathrm{C}_{p^{n-t}}$. 故 t 也是不变量. 由这些事实可得定理结论. □

表 13.1

G	(A1)	(A2)	(A3)	(A4)
$\lvert G'\rvert$	p^r	p^{r+n-t}	p^{r+m-s}	p^{r+m-s}
G/G'	$\mathrm{C}_{p^m} \times \mathrm{C}_{p^n}$	$\mathrm{C}_{p^m} \times \mathrm{C}_{p^t}$	$\mathrm{C}_{p^s} \times \mathrm{C}_{p^n}$	$\mathrm{C}_{p^{n+s-t}} \times \mathrm{C}_{p^t}$

下面我们分类内 $\mathcal{P}_2$-p 群. 由定理 13.3.11 可知, $G_3 \cong \mathrm{C}_p$ 或 C_p^2. 下面总假设 $p > 3$. 分这两种大的情况讨论.

13.4.1 $G_3 \cong \mathrm{C}_p$ 的情形

若 G 是亚循环的, 通过检验定理 6.1.3 即得如下定理.

定理 13.4.3 设 G 是奇数阶亚循环 p 群. 则 G 是内 $\mathcal{P}_2$-p 群当且仅当 G 与下列群同构:

$$\langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, [a, b] = a^{p^r}\rangle,$$

其中 r, s, t, u 是非负整数满足 $r \geqslant 1, u \leqslant r$ 且 $s + u = r + 1$. 参数 r, s, t 和 u 的不同值给出不同构的群.

定理 13.4.4 设 G 是非亚循环 p 群. 若 $G_3 \cong \mathrm{C}_p$, 则 G 是内 $\mathcal{P}_2$-p 群当且仅当 G 同构于下列互不同构的群之一.

(A) $m \geqslant n \geqslant r \geqslant 1$.

(A1) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = 1, [c, a] = x, [c, b] = 1 \rangle$;

(A2) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = 1, [c, a] = 1, [c, b] = x \rangle$, $m > n$;

(A3) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = x, [c, a] = x, [c, b] = 1 \rangle$, $n > r$;

(A4) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = x, [c, a] = 1, [c, b] = x \rangle$, $m > n > r$;

(A5) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = x, [a, b] = c, c^{p^r} = 1, [c, a] = x^{u_1}, [c, b] = 1 \rangle$, $u_1 = 1$ 或 λ, $m > n$;

(A6) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = x, [a, b] = c, c^{p^r} = 1, [c, a] = 1, [c, b] = x \rangle$, $m > n$;

(A7) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = x, [a, b] = c, c^{p^r} = x, [c, a] = x^{u_1}, [c, b] = 1 \rangle$, $1 \leqslant u_1 \leqslant p - 1$, $m > n > r$;

(A8) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = x, [a, b] = c, c^{p^r} = x, [c, a] = 1, [c, b] = x \rangle$, $m > n > r$;

(A9) $\langle a, b, c, x \mid a^{p^m} = x, b^{p^n} = 1, [a, b] = c, c^{p^r} = 1, [c, a] = x, [c, b] = 1 \rangle$;

(A10) $\langle a, b, c, x \mid a^{p^m} = x, b^{p^n} = 1, [a, b] = c, c^{p^r} = 1, [c, a] = 1, [c, b] = x^{v_1} \rangle$, $v_1 = 1$ 或 λ;

(A11) $\langle a, b, c, x \mid a^{p^m} = x, b^{p^n} = 1, [a, b] = c, c^{p^r} = x, [c, a] = x, [c, b] = 1 \rangle$, $n > r$;

(A12) $\langle a, b, c, x \mid a^{p^m} = x, b^{p^n} = 1, [a, b] = c, c^{p^r} = x, [c, a] = 1, [c, b] = x^{v_1} \rangle, 1 \leqslant v_1 \leqslant p - 1, n > r$.

(B) $m \geqslant n > r \geqslant 1$, $n > t \geqslant (n + r)/2$.

(B1) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = b^{p^t}, [c, a] = x, [c, b] = 1 \rangle$;

(B2) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = b^{p^t}, [c, a] = 1, [c, b] = x \rangle$;

(B3) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = b^{p^t} x, [c, a] = x^u, [c, b] = 1 \rangle$, $1 \leqslant u \leqslant p - 1$;

(B4) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = b^{p^t} x, [c, a] = 1, [c, b] = x \rangle$;

(B5) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = x, [a, b] = c, c^{p^r} = b^{p^t}, [c, a] = x^u, [c, b] = 1 \rangle$, $1 \leqslant u \leqslant p - 1$, $t > (n + r)/2$;

(B6) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = x, [a, b] = c, c^{p^r} = b^{p^t}, [c, a] = 1, [c, b] = x \rangle$, $t > (n + r)/2$;

(B7) $\langle a, b, c, x \mid a^{p^m} = 1, b^{p^n} = x, [a, b] = c, c^{p^r} = b^{p^t}, [c, a] = x^u, [c, b] = x \rangle$, $1 \leqslant u \leqslant p - 1$, $m = n$, $t > (n + r)/2$;

(B8) $\langle a, b, c, x \mid a^{p^m} = x, b^{p^n} = 1, [a, b] = c, c^{p^r} = b^{p^t}, [c, a] = x, [c, b] = 1 \rangle$;

(B9) $\langle a, b, c, x \mid a^{p^m} = x, b^{p^n} = 1, [a, b] = c, c^{p^r} = b^{p^t}, [c, a] = 1, [c, b] = x^{v_1} \rangle$, $v_1 = 1$ 或 λ;

(B10) $\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=x, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x^{u_1}, [c,b]=1\rangle$, $1\leqslant u_1\leqslant p-1$, $m>n$, $t>(n+r)/2$;

(B11) $\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=x, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=1, [c,b]=x^{v_1}\rangle$, $1\leqslant v_1\leqslant p-1$, $m>n$, $t>(n+r)/2$.

(C) $m>n>r\geqslant 1$, $m>s\geqslant (m+r)/2$, $n\geqslant m+r-s$.

(C1) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=x, [c,b]=1\rangle$;

(C2) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=1, [c,b]=x\rangle$;

(C3) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=x, [c,b]=x\rangle$, $s<n$;

(C4) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}x, [c,a]=x, [c,b]=1\rangle$;

(C5) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}x, [c,a]=1, [c,b]=x^v\rangle$, $1\leqslant v\leqslant p-1$;

(C6) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}x, [c,a]=x, [c,b]=x^v\rangle$, $1\leqslant v\leqslant p-1$, $s<n$;

(C7) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=x, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=x^{u_2}, [c,b]=1\rangle$, $u_2=1$ 或 λ;

(C8) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=x, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=x^{u_2}, [c,b]=x\rangle$, $0\leqslant u_2\leqslant p-1$, $s\leqslant n$;

(C9) $=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=x, [a,b]=c, c^{p^r}=a^{p^s}x, [c,a]=x^{u_1}, [c,b]=1\rangle$, $1\leqslant u_1\leqslant p-1$, $s>n$;

(C10) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=x, [a,b]=c, c^{p^r}=a^{p^s}x^{k_1}, [c,a]=1, [c,b]=x\rangle$, $0\leqslant k_1\leqslant p-1$, $s>n$;

(C11) $\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=x, [c,b]=1\rangle$, $s>(m+r)/2$, $n>m+r-s$;

(C12) $\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=1, [c,b]=x^v\rangle$, $1\leqslant v\leqslant p-1$, $s>(m+r)/2$, $n>m+r-s$;

(C13) $\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=x, [c,b]=x^v\rangle$, $1\leqslant v\leqslant p-1$, $s>(m+r)/2$, $n>m+r-s$, $s<n$.

(D) $m>n>r\geqslant 1$, $m>s>t>r, s+n<m+t, n>t\geqslant m-s+r$.

(D1) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=x, [c,b]=1\rangle$;

(D2) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=1, [c,b]=x\rangle$;

(D3) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}x, [c,a]=x^u, [c,b]=1\rangle$, $1\leqslant u\leqslant p-1$;

(D4) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}x, [c,a]=1, [c,b]=x^v\rangle$, $1\leqslant v\leqslant p-1$;

(D5) $\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=x, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=x^u, [c,b]=1\rangle$, $1\leqslant u\leqslant p-1$;

(D6) $\langle a,b,c \mid a^{p^m}=1, b^{p^n}=x, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=1, [c,b]=x^v\rangle$, $1\leqslant v\leqslant p-1$;

(D7) $\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=x^u, [c,b]=1\rangle$, $1\leqslant u\leqslant p-1, t>m-s+r$;

(D8) $\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=1, [c,b]=x^v\rangle$, $1\leqslant v\leqslant p-1, t>m-s+r$.

在定理的陈述中，λ 是一个固定的模 p 的平方非剩余，且在每个群中，$x^p=[x,a]=[x,b]=1$ 被省略. 定理中所有的群均为阶 $p^{m+n+r+1}$.

证明 因为 G 非亚循环，由定理 2.5.3 可得，$G/\Phi(G')G_3$ 非亚循环. 因而 G/G_3 非亚循环. 令 $\overline{G}=G/G_3$. 因为 $p>3$，由定理 13.3.11(1) 可知，$d(\overline{G})=2$ 且 $c(\overline{G})=2$. 则 $\overline{G}$ 同构于定理 13.4.2 中的群之一. 由定理 13.3.4 可知 $c(G)=3$. 由此可得 $G_3\leqslant Z(G)$. 于是 G 是 $\overline{G}$ 被 G_3 的中心扩张. 下面分情况讨论.

令 $G_3=\langle x\rangle$. 为方便，在下列陈述中，λ 是一个固定的模 p 的平方非剩余，且在群的定义关系中，$x^p=[x,a]=[x,b]=1$ 被省略.

情形 (A) G/G_3 同构于定理 13.4.2 中的群 (A1).

令 $G/G_3\cong\langle \bar{a},\bar{b},\bar{c} \mid \bar{a}^{p^m}=1, \bar{b}^{p^n}=1, [\bar{a},\bar{b}]=\bar{c}, \bar{c}^{p^r}=1, [\bar{c},\bar{a}]=[\bar{c},\bar{b}]=1\rangle$，其中 $m\geqslant n\geqslant r\geqslant 1$. 则可设

$$G=\langle a,b,c,x \mid a^{p^m}=x^i, b^{p^n}=x^j, [a,b]=cx^k, c^{p^r}=x^l, [c,a]=x^u, [c,b]=x^v\rangle,$$

其中

$$i,j,k,l,u,v\in\{i\in\mathbf{Z} \mid 0\leqslant i\leqslant p-1\}.$$

用 c 替换 cx^k 可得

$$G=\langle a,b,c,x \mid a^{p^m}=x^i, b^{p^n}=x^j, [a,b]=c, c^{p^r}=x^l, [c,a]=x^u, [c,b]=x^v\rangle.$$

下面分五种子情况讨论.

(1) $a^{p^m}=1, b^{p^n}=1$ 且 $c^{p^r}=1$.

此时，$G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=1, [c,a]=x^u, [c,b]=x^v\rangle$. 若 $[c,b]=1$，用 x 替换 x^u 即得群 (A1).

若 $[c,b]\neq 1$，不妨设

$$G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=1, [c,a]=x^u, [c,b]=x\rangle.$$

用 a 替换 $b^{-u}a$ 可得

$$G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=1, [c,a]=1, [c,b]=x\rangle.$$

若 $m=n$, 用 b 替换 a, a 替换 b, c 替换 c^{-1}, x 替换 x^{-1} 可得

$$G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=1, [c,a]=x, [c,b]=1\rangle.$$

此时 G 与群 (A1) 同构. 若 $m>n$. 我们得到群 (A2).

(2) $a^{p^m}=1, b^{p^n}=1$ 且 $c^{p^r}\neq 1$.

不妨设 $G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=x, [c,a]=x^u, [c,b]=x^v\rangle$. 因为 $1=[a,b^{p^n}]=c^{p^n}$, 故 $n>r$.

若 $[c,b]=1$, 则

$$G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=x, [c,a]=x^u, [c,b]=1\rangle.$$

明显地, $x^u\neq 1$. 于是存在 h 使得 $hu\equiv 1 (\mathrm{mod}\ p)$. 用 a 替换 a^h, c 替换 $[a^h,b]$, x 替换 x^h 即得群 (A3).

若 $[c,b]\neq 1$, 则

$$G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=x, [c,a]=x^u, [c,b]=x^v\rangle.$$

于是存在 h 使得 $vh\equiv -u (\mathrm{mod}\ p)$. 用 a 替换 $b^h a$ 可得

$$G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=x, [c,a]=1, [c,b]=x^v\rangle.$$

则存在 h_1 使得 $vh_1\equiv 1 (\mathrm{mod}\ p)$. 再用 b 替换 b^{h_1}, c 替换 $[a,b^{h_1}]$, x 替换 x^{h_1} 可得

$$G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=x, [c,a]=1, [c,b]=x\rangle.$$

若 $m=n$, 用 b 替换 a, a 替换 b, c 替换 c^{-1}, x 替换 x^{-1} 可得

$$G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=x, [c,a]=x, [c,b]=1\rangle.$$

此时 G 与群 (A3) 同构. 若 $m>n$. 我们得到群 (A4).

(3) $a^{p^m}=1$, $b^{p^n}\neq 1$ 且 $m>n$.

不妨设

$$G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=x, [a,b]=c, c^{p^r}=x^k, [c,a]=x^u, [c,b]=x^v\rangle.$$

(3-1) $c^{p^r}=1$.

此时 $G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=x, [a,b]=c, c^{p^r}=1, [c,a]=x^u, [c,b]=x^v\rangle$.

若 $[c,b]=1$, 则

$$G=\langle a,b,c,x \mid a^{p^m}=1, b^{p^n}=x, [a,b]=c, c^{p^r}=1, [c,a]=x^u, [c,b]=1\rangle.$$

于是存在 h 使得 $h^2u \equiv 1$ 或 λ. 令 $u_1 = h^2u$. 用 a 替换 a^h, c 替换 $[a^h, b]$ 即得群 (A5).

若 $[c,b] \neq 1$, 则

$$G = \langle a,b,c,x \mid a^{p^m} = 1, b^{p^n} = x, [a,b] = c, c^{p^r} = 1, [c,a] = x^u, [c,b] = x^v \rangle.$$

于是存在 h 使得 $vh \equiv -u (\mathrm{mod}\ p)$. 用 a 替换 $b^h a$ 即得

$$G = \langle a,b,c,x \mid a^{p^m} = 1, b^{p^n} = x, [a,b] = c, c^{p^r} = 1, [c,a] = 1, [c,b] = x^v \rangle.$$

再用 a 替换 a^v, c 替换 $[a^v, b]$ 即得群 (A6).

(3-2) $c^{p^r} \neq 1$.

此时, $G = \langle a,b,c,x \mid a^{p^m} = 1, b^{p^n} = x, [a,b] = c, c^{p^r} = x^k, [c,a] = x^u, [c,b] = x^v \rangle$. 令 $u_1 = k^2u$ 且 $v_1 = kv$. 用 a 替换 a^k, 用 c 替换 $[a^k, b]$ 即得

$$G = \langle a,b,c,x \mid a^{p^m} = 1, b^{p^n} = x, [a,b] = c, c^{p^r} = x, [c,a] = x^{u_1}, [c,b] = x^{v_1} \rangle.$$

因为 $c^{p^n} = [a, b^{p^n}] = 1$, 故 $n > r$. 若 $[c,b] = 1$, 我们得到群 (A7).

若 $[c,b] \neq 1$, 则

$$G = \langle a,b,c,x \mid a^{p^m} = 1, b^{p^n} = x, [a,b] = c, c^{p^r} = x, [c,a] = x^{u_1}, [c,b] = x^{v_1} \rangle.$$

于是存在 h 使得 $v_1 h \equiv -u_1 (\mathrm{mod}\ p)$. 用 a 替换 $b^h a$, 即得

$$G = \langle a,b,c,x \mid a^{p^m} = 1, b^{p^n} = x, [a,b] = c, c^{p^r} = x, [c,a] = 1, [c,b] = x^{v_1} \rangle.$$

又存在 h_1 使得 $v_1 h_1 \equiv 1 (\mathrm{mod}\ p)$. 再用 b 替换 b^{h_1}, c 替换 $[a, b^{h_1}]$, x 替换 x^{h_1} 即得群 (A8).

(4) $a^{p^m} \neq 1$.

不妨设

$$G = \langle a,b,c,x \mid a^{p^m} = x, b^{p^n} = x^j, [a,b] = c, c^{p^r} = x^k, [c,a] = x^u, [c,b] = x^v \rangle.$$

因为 $c^{p^n} = [a, b^{p^n}] = 1$, 故 $p^n \geqslant \exp(G')$. 由定理 1.1.10 易得 G 是 p^n 交换的. 令 $x^{v_1} = [c, a^{-jp^{m-n}} b]$. 用 b 替换 $a^{-jp^{m-n}} b$ 即得

$$G = \langle a,b,c,x \mid a^{p^m} = x, b^{p^n} = 1, [a,b] = c, c^{p^r} = x^k, [c,a] = x^u, [c,b] = x^{v_1} \rangle.$$

(4-1) $k = 0$.

此时, $G = \langle a,b,c,x \mid a^{p^m} = x, b^{p^n} = 1, [a,b] = c, c^{p^r} = 1, [c,a] = x^u, [c,b] = x^v \rangle$.

若 $[c,b]=1$, 则

$$G=\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=1, [c,a]=x^u, [c,b]=1\rangle.$$

于是存在 h 使得 $uh\equiv 1(\bmod p)$. 用 a 替换 a^h, c 替换 $[a^h,b]$, x 替换 x^h 即得群 (A9).

若 $[c,b]\neq 1$, 则

$$G=\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=1, [c,a]=x^u, [c,b]=x^v\rangle.$$

于是存在 h 使得 $hv\equiv -u(\bmod p)$. 用 a 替换 $b^h a$ 即得

$$G=\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=1, [c,a]=1, [c,b]=x^v\rangle.$$

又存在 h_1 使得 ${h_1}^2v\equiv 1$ 或 λ. 令 $v_1={h_1}^2v$. 用 b 替换 b^{h_1}, c 替换 $[a,b^{h_1}]$ 即得群 (A10).

(4-2) $k\neq 0$.

此时, $G=\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=x^k, [c,a]=x^u, [c,b]=x^v\rangle$. 因为 $c^{p^n}=[a,b^{p^n}]=1$, 故 $n>r$. 由定理 1.1.10 易得 G 是 p^n 交换的. 于是存在 h 使得 $hk\equiv 1(\bmod p)$. 令 $u_1=hu$ 且 $v_1=h^2v$. 用 b 替换 b^h, c 替换 $[a,b^h]$ 即得

$$G=\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=x, [c,a]=x^{u_1}, [c,b]=x^{v_1}\rangle.$$

若 $[c,b]=1$, 则

$$G=\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=x, [c,a]=x^{u_1}, [c,b]=1\rangle.$$

于是存在 h 使得 $hu_1\equiv 1(\bmod p)$. 用 a 替换 a^h, c 替换 $[a^h,b]$, x 替换 x^h 即得群 (A11).

若 $[c,b]\neq 1$, 则

$$G=\langle a,b,c,x \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=x, [c,a]=x^{u_1}, [c,b]=x^{v_1}\rangle.$$

于是存在 h 使得 $v_1h\equiv -u_1(\bmod p)$. 用 a 替换 $b^h a$ 即得群 (A12).

(5) $a^{p^m}=1$, $b^{p^n}\neq 1$ 且 $m=n$.

此时, $G=\langle a,b,c,x \mid a^{p^m}=x^i, b^{p^n}=x^j, [a,b]=c, c^{p^r}=x^l, [c,a]=x^u, [c,b]=x^v\rangle$. 用 b 替换 a, a 替换 b, c 替换 c^{-1}, x 替换 x^{-1}, 这归结为情形 (4).

下面以群 (A12) 为例证明定理中的群具有阶 $p^{m+n+r+1}$. 设 G 是群 (A12), $H=\langle a,c\rangle<G$. 则 $H\cong \mathrm{C}_{p^{m+1}}\times \mathrm{C}_{p^r}$. 令 $\sigma(g):h\longrightarrow h^g$, 其中 $h\in H$, $g\in G$. 则

$\sigma(b) \in \mathrm{Aut}(H)$ 且 $\sigma^{p^n}(b) = \sigma(1)$. 因为 $b^{p^{n-1}} \notin H$ 且 $b^{p^n} = 1 \in H$, 故 G 是 H 被 C_{p^n}. 于是 $|G| = p^{m+n+r+1}$.

对于 G/G_3 的其余情形, 类似于上述情形的论证可得定理中的其他群. 进一步可证定理中的群满足假设的条件且两两互不同构. 欲知其详, 读者可参看文献 [125]. □

13.4.2 $G_3 \cong \mathrm{C}_p^2$ 的情形

定理 13.4.5 设 G 是有限 p 群. 若 $G_3 \cong \mathrm{C}_p^2$, 则 G 是内 $\mathcal{P}_2$-p 群当且仅当 G 同构于下列互不同构的群之一.

(A) $m \geqslant n \geqslant r \geqslant 1$. 若 $c^{p^r} \neq 1$, 则 $n > r$.

(A1) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = 1, [c, a] = x, [c, b] = y\rangle$;

(A2) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = y, [c, a] = x, [c, b] = y\rangle$;

(A3) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = x, [c, a] = x, [c, b] = y\rangle$, $m > n$;

(A4) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = y, [a, b] = c, c^{p^r} = 1, [c, a] = x, [c, b] = y\rangle$;

(A5) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = y, [a, b] = c, c^{p^r} = y, [c, a] = x, [c, b] = y\rangle$;

(A6) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = y, [a, b] = c, c^{p^r} = x, [c, a] = x, [c, b] = y\rangle$, $m > n$;

(A7) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = y, [a, b] = c, c^{p^r} = xy^{k_4}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant k_4 \leqslant p-1$, $m = n$;

(A8) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = x^{j_3}, [a, b] = c, c^{p^r} = 1, [c, a] = x, [c, b] = y\rangle$, $j_3 = 1$ 或 λ;

(A9) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = x^{j_3}, [a, b] = c, c^{p^r} = x, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant j_3 \leqslant p-1$;

(A10) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = x^{j_3}, [a, b] = c, c^{p^r} = xy, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant j_3 \leqslant p-1$;

(A11) $\langle a, b, c, x, y \mid a^{p^m} = y^{i_3}, b^{p^n} = 1, [a, b] = c, c^{p^r} = 1, [c, a] = x, [c, b] = y\rangle$, $i_3 = 1$ 或 λ, $m > n$;

(A12) $\langle a, b, c, x, y \mid a^{p^m} = y^{i_3}, b^{p^n} = 1, [a, b] = c, c^{p^r} = y, [c, a] = x, [c, b] = y\rangle$, $i_3 = 1$ 或 λ, $m > n$;

(A13) $\langle a, b, c, x, y \mid a^{p^m} = y^{i_3}, b^{p^n} = 1, [a, b] = c, c^{p^r} = x, [c, a] = x, [c, b] = y\rangle$, $i_3 = 1$ 或 λ, $m > n$;

(A14) $\langle a, b, c, x, y \mid a^{p^m} = x, b^{p^n} = 1, [a, b] = c, c^{p^r} = 1, [c, a] = x, [c, b] = y\rangle$, $m > n$;

(A15) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=y, [c,a]=x, [c,b]=y\rangle$, $m>n$;

(A16) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=xy^{k_5}, [c,a]=x, [c,b]=y\rangle$, $0\leqslant k_5\leqslant p-1$, $m>n$;

(A17) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=1, [c,a]=y^{u_3}, [c,b]=x^{v_3}\rangle$, $u_3=1$ 或 λ, $v_3=1$ 或 λ, $m>n$;

(A18) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=x, [c,a]=y^{u_4}, [c,b]=x^{v_1}\rangle$, $1\leqslant v_1\leqslant p-1$, $u_4=1$ 或 λ, $m>n$;

(A19) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=y, [c,a]=y^{u_3}, [c,b]=x^{v_3}\rangle$, $1\leqslant u_3\leqslant p-1$, $v_3=1$ 或 λ, $m>n$;

(A20) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=1, [c,a]=x, [c,b]=y^{v_3}\rangle$, $1\leqslant v_3\leqslant p-1$, $m>n$;

(A21) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=y, [c,a]=x, [c,b]=y^{v_4}\rangle$, $1\leqslant v_4\leqslant p-1$, $m>n$;

(A22) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=xy^{k_5}, [c,a]=x, [c,b]=y^{v_4}\rangle$, $0\leqslant k_5\leqslant p-1$, $1\leqslant v_4\leqslant p-1$, $m>n$;

(A23) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=y, [c,a]=x, [c,b]=y^{v_3}\rangle$, $1\leqslant v_3\leqslant p-1$, $m=n$;

(A24) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=y, [c,a]=xy^{u_4}, [c,b]=y\rangle$, $1\leqslant u_4\leqslant p-1$, $m=n$;

(A25) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=y, [c,a]=y^{u_4}, [c,b]=x^{v_5}\rangle$, $1\leqslant u_4\leqslant p-1$, $v_5=1$ 或 λ, $m=n$;

(A26) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=y, [c,a]=y^{u_4}, [c,b]=x^{v_6}y\rangle$, $1\leqslant u_4\leqslant p-1$, $1\leqslant v_6\leqslant p-1$, $m=n$;

(A27) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=1, [c,a]=x, [c,b]=y\rangle$, $m=n$;

(A28) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=1, [c,a]=y^{-1}, [c,b]=xy^{v_3}\rangle$, $0\leqslant v_3\leqslant p-1/2$, $m=n$;

(A29) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=1, [c,a]=y^{-1}, [c,b]=x^{\lambda}y^{v_3}\rangle$, $0\leqslant v_3\leqslant p-1/2$, $m=n$;

(A30) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=y, [a,b]=c, c^{p^r}=1, [c,a]=y^{-\lambda}, [c,b]=x^{\lambda}y^{2\lambda}\rangle$, $m=n$.

(B) $m\geqslant n>r\geqslant 1$, $n>t\geqslant (n+r)/2$.

(B1) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$;

(B2) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=b^{p^t}y, [c,a]=x, [c,b]=y\rangle$;

(B3) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=b^{p^t}x^{k_1}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant k_1\leqslant p-1$;

(B4) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=y, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $2t>n+r$;

(B5) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=y, [a,b]=c, c^{p^r}=b^{p^t}x^{k_1}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant k_1\leqslant p-1$, $2t>n+r$;

(B6) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=x^{j_1}, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_1\leqslant p-1$, $2t>n+r$, $m>n$;

(B7) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=x^{j_1}, [a,b]=c, c^{p^r}=b^{p^t}y, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_1\leqslant p-1$, $2t>n+r$, $m>n$;

(B8) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=x^{j_1}, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_1\leqslant p-1$, $m=n$, $2t>n+r$;

(B9) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=x^{j_1}y, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_1\leqslant p-1$, $m=n$, $2t>n+r$;

(B10) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=x^{j_1}y^{j_2}, [a,b]=c, c^{p^r}=b^{p^t}y, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_1\leqslant p-1$, $0\leqslant j_2\leqslant p-1$, $2t>n+r$, $m=n$;

(B11) $\langle a,b,c,x,y \mid a^{p^m}=y^{i_3}, b^{p^n}=1, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $i_3=1$ 或 λ;

(B12) $\langle a,b,c,x,y \mid a^{p^m}=y^{i_3}, b^{p^n}=1, [a,b]=c, c^{p^r}=b^{p^t}x^{k_1}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant k_1\leqslant p-1$, $i_3=1$ 或 λ;

(B13) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$;

(B14) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=1, [a,b]=c, c^{p^r}=b^{p^t}y^{k_4}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant k_4\leqslant p-1$;

(B15) $\langle a,b,c,x,y \mid a^{p^m}=y^{i_3}, b^{p^n}=y, [a,b]=c, c^{p^r}=b^{p^t}x^{k_1}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant i_3\leqslant p-1$, $1\leqslant k_1\leqslant p-1$, $m>n$, $2t>n+r$;

(B16) $\langle a,b,c,x,y \mid a^{p^m}=y^{i_3}, b^{p^n}=y, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant i_3\leqslant p-1$, $m>n$, $2t>n+r$;

(B17) $\langle a,b,c,x,y \mid a^{p^m}=y^{i_3}, b^{p^n}=x^{j_1}, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $m=n$, $2t>n+r$, $i_3=1$ 或 λ;

(B18) $\langle a,b,c,x,y \mid a^{p^m}=y^{i_4}, b^{p^n}=x^{j_1}y, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant i_4\leqslant p-1$, $1\leqslant j_1\leqslant p-1$, $m=n$, $2t>n+r$;

(B19) $\langle a,b,c,x,y \mid a^{p^m}=y^{i_3}, b^{p^n}=x^{j_1}, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_1\leqslant p-1$, $m>n$, $2t>n+r$, $i_3=1$ 或 λ;

(B20) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=x^{j_1}y^{j_4}, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $0\leqslant j_1\leqslant p-1$, $1\leqslant j_4\leqslant p-1$, $m>n$, $2t>n+r$;

(B21) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=x^{j_1}, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_1\leqslant p-1$, $m>n$, $2t>n+r$;

(B22) $\langle a,b,c,x,y \mid a^{p^m}=x, b^{p^n}=x^{j_1}, [a,b]=c, c^{p^r}=b^{p^t}y^{k_4}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_1\leqslant p-1$, $1\leqslant k_4\leqslant p-1$, $m>n$, $2t>n+r$;

(B23) $\langle a,b,c,x,y \mid a^{p^m}=x^{i_3}, b^{p^n}=y, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant i_3\leqslant p-1$, $m=n$, $2t>n+r$;

(B24) $\langle a,b,c,x,y \mid a^{p^m}=xy^{i_3}, b^{p^n}=y, [a,b]=c, c^{p^r}=b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant i_3\leqslant p-1$, $m=n$, $2t>n+r$.

(C) $m>n>r\geqslant 1$, $m>s\geqslant (m+r)/2$, $n\geqslant m+r-s$.

(C1) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=x, [c,b]=y\rangle$;

(C2) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}y^{k_2}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant k_2\leqslant p-1$;

(C3) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}x, [c,a]=x, [c,b]=y\rangle$, $s\geqslant n$;

(C4) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}xy^{k_2}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant k_2\leqslant p$, $s<n$;

(C5) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=y, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=x, [c,b]=y\rangle$, $s\leqslant n$;

(C6) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=y, [a,b]=c, c^{p^r}=a^{p^s}y^{k_2}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant k_2\leqslant p$, $s>n$;

(C7) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=y, [a,b]=c, c^{p^r}=a^{p^s}x^{k_3}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant k_3\leqslant p-1$;

(C8) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=x^{j_3}, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=x, [c,b]=y\rangle$, $j_3=1$ 或 λ;

(C9) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=x^{j_3}, [a,b]=c, c^{p^r}=a^{p^s}y^{k_3}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant k_3\leqslant p-1$, $j_3=1$ 或 λ;

(C10) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=x^{j_3}y, [a,b]=c, c^{p^r}=a^{p^s}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_3\leqslant p-1$, $s\leqslant n$;

(C11) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=x^{j_3}y, [a,b]=c, c^{p^r}=a^{p^s}y^{k_3}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_3\leqslant p-1$, $1\leqslant k_3\leqslant p-1$, $s\leqslant n$;

(C12) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=x^{j_4}, [a,b]=c, c^{p^r}=a^{p^s}x, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_4\leqslant p-1$, $s>n$;

(C13) $\langle a,b,c,x,y \mid a^{p^m}=1, b^{p^n}=x^{j_4}, [a,b]=c, c^{p^r}=a^{p^s}xy^{k_3}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant j_4\leqslant p-1$, $1\leqslant k_3\leqslant p-1$, $s>n$;

(C14) $\langle a, b, c, x, y \mid a^{p^m} = y^{i_2}, b^{p^n} = 1, [a, b] = c, c^{p^r} = a^{p^s}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant i_2 \leqslant p-1$, $s > m+r-s$, $n > m+r-s$;

(C15) $\langle a, b, c, x, y \mid a^{p^m} = y^{i_2}, b^{p^n} = x^{j_3}, [a, b] = c, c^{p^r} = a^{p^s}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant i_2 \leqslant p-1$, $s > m+r-s$, $n > m+r-s$, $j_3 = 1$ 或 λ;

(C16) $\langle a, b, c, x, y \mid a^{p^m} = y^{i_2}, b^{p^n} = 1, [a, b] = c, c^{p^r} = a^{p^s}x, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant i_2 \leqslant p-1$, $s > m+r-s$, $n > m+r-s$;

(C17) $\langle a, b, c, x, y \mid a^{p^m} = y^{i_2}, b^{p^n} = x^{j_3}, [a, b] = c, c^{p^r} = a^{p^s}x, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant i_2 \leqslant p-1$, $1 \leqslant j_3 \leqslant p-1$, $n < s$, $s > m+r-s$, $n > m+r-s$;

(C18) $\langle a, b, c, x, y \mid a^{p^m} = x, b^{p^n} = 1, [a, b] = c, c^{p^r} = a^{p^s}, [c, a] = x, [c, b] = y\rangle$, $s > m+r-s$, $n > m+r-s$;

(C19) $\langle a, b, c, x, y \mid a^{p^m} = xy^{i_2}, b^{p^n} = 1, [a, b] = c, c^{p^r} = a^{p^s}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant i_2 \leqslant p-1$, $s < n$, $s > m+r-s$, $n > m+r-s$;

(C20) $\langle a, b, c, x, y \mid a^{p^m} = x, b^{p^n} = 1, [a, b] = c, c^{p^r} = a^{p^s}y^{k_3}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant k_3 \leqslant p-1$, $s > m+r-s$, $n > m+r-s$;

(C21) $\langle a, b, c, x, y \mid a^{p^m} = xy^{i_2}, b^{p^n} = 1, [a, b] = c, c^{p^r} = a^{p^s}y^{k_3}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant i_2 \leqslant p-1$, $1 \leqslant k_3 \leqslant p-1$, $s < n$, $s > m+r-s$, $n > m+r-s$;

(C22) $\langle a, b, c, x, y \mid a^{p^m} = xy^{i_2}, b^{p^n} = y^{j_4}, [a, b] = c, c^{p^r} = a^{p^s}, [c, a] = x, [c, b] = y\rangle$, $0 \leqslant i_2 \leqslant p-1$, $1 \leqslant j_4 \leqslant p-1$, $n \geqslant s$, $s > m+r-s$, $n > m+r-s$;

(C23) $\langle a, b, c, x, y \mid a^{p^m} = x, b^{p^n} = y^{j_4}, [a, b] = c, c^{p^r} = a^{p^s}y^{k_3}, [c, a] = x, [c, b] = y\rangle$, $0 \leqslant k_3 \leqslant p-1$, $1 \leqslant j_4 \leqslant p-1$, $n < s$, $s > m+r-s$, $n > m+r-s$.

(D) $m > n > r \geqslant 1$, $m > s > t > r$, $s+n < m+t$, $n > t \geqslant m-s+r$.

(D1) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = a^{p^s}b^{p^t}, [c, a] = x, [c, b] = y\rangle$;

(D2) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = a^{p^s}b^{p^t}y^{k_2}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant k_2 \leqslant p-1$;

(D3) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = 1, [a, b] = c, c^{p^r} = a^{p^s}b^{p^t}x^{k_1}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant k_1 \leqslant p-1$;

(D4) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = y^{j_2}, [a, b] = c, c^{p^r} = a^{p^s}b^{p^t}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant k_2 \leqslant p-1$;

(D5) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = y^{j_2}, [a, b] = c, c^{p^r} = a^{p^s}b^{p^t}x^{k_1}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant j_2 \leqslant p-1$, $1 \leqslant k_1 \leqslant p-1$;

(D6) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = x^{j_1}, [a, b] = c, c^{p^r} = a^{p^s}b^{p^t}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant j_1 \leqslant p-1$;

(D7) $\langle a, b, c, x, y \mid a^{p^m} = 1, b^{p^n} = x^{j_1}, [a, b] = c, c^{p^r} = a^{p^s}b^{p^t}y^{k_3}, [c, a] = x, [c, b] = y\rangle$, $1 \leqslant j_1 \leqslant p-1$, $1 \leqslant k_3 \leqslant p-1$;

(D8) $\langle a,b,c,x,y \mid a^{p^m}=y^{i_2}, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant i_2\leqslant p-1$, $t>m-s+r$;

(D9) $\langle a,b,c,x,y \mid a^{p^m}=y^{i_2}, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}x^{k_1}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant i_2\leqslant p-1$, $1\leqslant k_1\leqslant p-1$, $t>m-s+r$;

(D10) $\langle a,b,c,x,y \mid a^{p^m}=y^{i_2}, b^{p^n}=x^{j_1}, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant i_2\leqslant p-1$, $1\leqslant j_1\leqslant p-1$, $t>m-s+r$;

(D11) $\langle a,b,c,x,y \mid a^{p^m}=x^{i_1}, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant i_1\leqslant p-1$, $t>m-s+r$;

(D12) $\langle a,b,c,x,y \mid a^{p^m}=x^{i_1}, b^{p^n}=1, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}y^{k_4}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant i_1\leqslant p-1, 1\leqslant k_4\leqslant p-1, t>m-s+r$;

(D13) $\langle a,b,c,x,y \mid a^{p^m}=x^{i_1}, b^{p^n}=y^{j_3}, [a,b]=c, c^{p^r}=a^{p^s}b^{p^t}, [c,a]=x, [c,b]=y\rangle$, $1\leqslant i_1\leqslant p-1, 1\leqslant j_3\leqslant p-1, t>m-s+r$.

在定理的陈述中, λ 是一个固定的模 p 的平方非剩余, 且在每个群中, $x^p=y^p=[x,a]=[x,b]=[y,a]=[y,b]=1$ 被省略. 定理中群的阶为 $p^{m+n+r+2}$.

证明 因为 $G_3\cong \mathrm{C}_p^2$, 故 G 非亚循环. 由定理 2.5.3 可得, $G/\Phi(G')G_3$ 非亚循环. 因而 G/G_3 非亚循环. 令 $\overline{G}=G/G_3$. 因为 $p>3$, 由定理 13.3.11(1) 可知, $d(\overline{G})=2$ 且 $c(\overline{G})=2$. 则 $\overline{G}$ 同构于定理 13.4.2 中的群之一. 由定理 13.3.4 可知 $c(G)=3$. 由此可得 $G_3\leqslant Z(G)$. 于是 G 是 $\overline{G}$ 被 G_3 的中心扩张. 与定理 13.4.4 讨论的方法类似可得定理中的群. 证明细节略去. 有兴趣的读者可参看文献 [126]. □

第 14 章　关于有限 p 群的其他结果

有限 p 群研究领域的问题浩如烟海, 我国学者从不同角度对 p 的有关问题开展了研究, 获得了丰富的结果. 例如, p 群的幂结构、余次数、特征标的核, 正则 p 群的幂零类, p 核 p 群, p 群的子群交、子群补以及具有特定性质的 p 群的分类等, 见文献 [2], [5], [6], [12], [18], [50], [80], [122], [128], [132], [133], [183], [185]—[187], [207], [208], [222], [226], [230], [233], [234], [239], [258], [264], [266], [267], [270], [271], [276], [283], [285]. 本章介绍这方面的某些结果. 各节的次序依照论文发表时间编排.

14.1　有限 p 群的幂结构

Mann 在文献 [151],[154] 中深入研究了有限 p 群的幂结构. 他在 [151] 中考察了有限 p 群 G 的下述三个性质:

P_1 : 对任意正整数 n, $\mho_n(G)=\mho_{\{n\}}(G)$;

P_2 : 对任意正整数 n, $\Omega_n(G)=\Omega_{\{n\}}(G)$;

P_3 : 对任意正整数 n, $|G:\Omega_n(G)|=|\mho_n(G)|$.

他规定, 如果群 G 的每个截断 (即子群、商群和子群的商群的统称) 都有性质 $P_i(i=1,2,3)$, 就称 G 是 P_i 群; 而如果 G 同时是 P_i 群 $(i=1,2,3)$, 就称 G 是 P 群. 他证明了, P_3 群是 P_2 群, P_2 群是 P_1 群 (从而, P 群与 P_3 群等价). 反之不然. 我们知道, 正则 p 群必是 P 群 [77], 反之不然. 我们还知道, 当 $n\leqslant p$ 时, p^n 阶群是正则群, 而对每个素数 p, 都存在 p^{p+1} 阶非正则群.

徐明曜和杨燕昌在 [237] 中引入了一种新的幂结构性质, 即半 p 交换性.

定义 14.1.1　称有限 p 群 G 是半 p 交换群, 如果对任意的 $a,b\in G$, $a^p=b^p$ 的充要条件是 $(a^{-1}b)^p=1$.

他们指出, 有限 p 群 G 是正则 p 群, 当且仅当 G 的每个截断是半 p 交换的. 见 [237] 中的定理 1. 在文献 [237] 的基础上, 王汝楫在文献 [233] 引进了以下的幂结构性质.

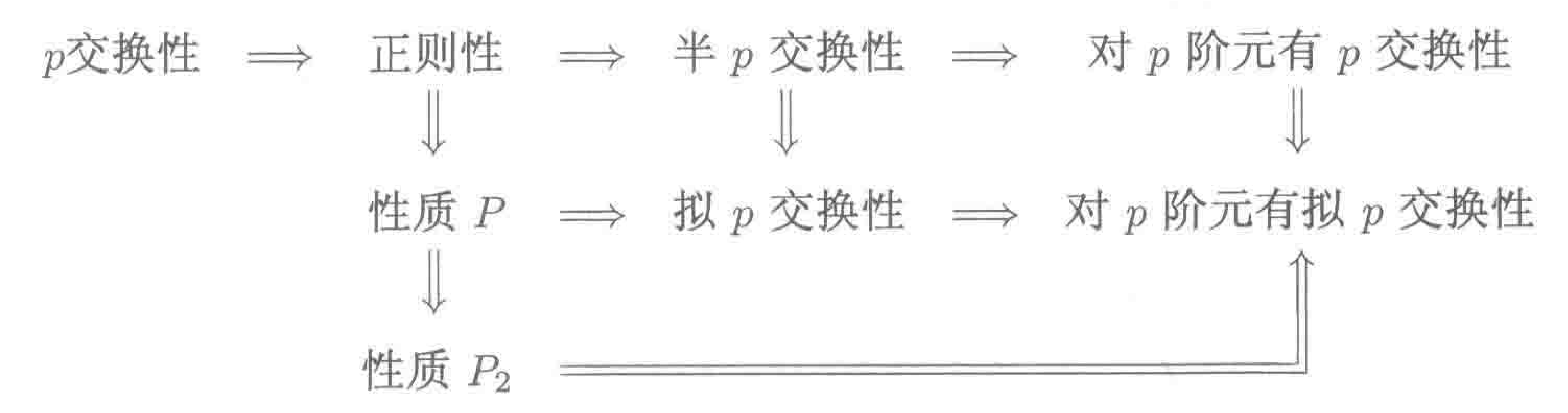
定义 14.1.2　称有限 p 群 G 是拟 p 交换群, 如果对任意的 $a,b\in G$, $\langle a^p\rangle=\langle b^p\rangle$ 的充要条件是存在 i,j 使得 $(a^ib^j)^p=1$, 其中 $ij\not\equiv 0(\mathrm{mod}\ p)$.

定义 14.1.3　称有限 p 群 G 对 p 阶元有拟 p 交换性, 如果对任意的 $a,b\in G$, 且 $b^p=1$, 有 $\langle (ab)^p\rangle=\langle a^p\rangle$.

定义 14.1.4 称有限 p 群 G 对 p 阶元有 p 交换性, 如果对任意的 $a, b \in G$, 且 $b^p = 1$, 有 $(ab)^p = a^p$.

他在文献 [233] 中考察了这三种 "交换性" 与性质 P、正则性之间的联系, 给出了 P 群和正则 p 群的几个充要条件. 另外, 他还在文献 [234] 考察了 p^{p+1} 阶亚交换的非正则 p 群的幂结构, 给出了它们是 P_i 群的充要条件. 作为应用, 还给出了包含一个交换的极大子群的 p^{p+1} 阶亚交换的非正则群的完全分类. 本节介绍他的工作.

由正则 p 群、P_i 的性质以及上述定义, 可得如下蕴涵关系:



进一步, 由例 14.1.9 并根据 [237] 中的定理 1 知, 对 p 阶元有 p 交换性确实比半 p 交换性弱; 根据下面的定理 14.1.6(3) 和定理 14.1.7(3) 知, 对 p 阶元有拟 p 交换性确实比对 p 阶元有 p 交换性弱; 由下面的命题 14.1.5 和定理 14.1.6(2) 知, 对 p 阶元有拟 p 交换性确实比拟 p 交换性弱; 例 14.1.8 表明, 拟 p 交换性 (从而对 p 阶元有拟 p 交换性) 不蕴涵性质 P_1. 由此知, 对 p 阶元有拟 p 交换性确实比性质 P_2 弱, 而拟 p 交换性确实比性质 P 弱; 由下面的定理 14.1.6(2) 和 [237] 中的定理 1 知, 拟 p 交换性确实比半 p 交换性弱; 定理 14.1.7 已指出, 半 p 交换性确实比正则性弱. 最后, 由下面的定理 14.1.7(4) 知, 拟 p 交换性与对 p 阶元有 p 交换性之间, 没有哪个性质蕴涵另一个性质.

显然, 上述四个定义中规定的 "交换性", 在取子群下保持. 但是, 它们在取商群下不一定保持. 事实上, 对半 p 交换性, [237] 已指出这一点. 若拟 p 交换性在取商群下保持, 由定理 14.1.6, 拟 p 交换性将与性质 P 等价, 这与上述拟 p 交换性确实比性质 P 弱相矛盾. 同样, 由命题 14.1.5 知, 对 p 阶元有拟 p 交换性, 在取商群下不一定保持. 例 14.1.10 表明, 对 p 阶元有 p 交换性, 在取商群下不一定保持.

首先介绍王汝楫上述定义的三种 "交换性" 与性质 P、正则性之间的联系及主要结果.

命题 14.1.5 有限 p 群 G 是 P_2 群当且仅当 G 的每个截断对 p 阶元有拟 p 交换性.

证明 由 [151] 中的推论 17 可知, 只需证充分性. 因为定理的条件是子商遗传的, 故使结论不真的最小阶反例 G 必是极小非 P_2 群. 由 [151] 中的定理 6

知, $G=\langle a,b\rangle$, $a^p=b^p=1$ 但 $(ab)^p\neq 1$. 利用 G 对 p 阶元有拟 p 交换性得 $\langle (ab)^p\rangle=\langle a^p\rangle=1$. 从而 $(ab)^p=1$. 矛盾. □

定理 14.1.6 设 G 是有限 p 群, 则下列陈述是等价的.

(1) G 是 P 群;

(2) G 的每个截断都是拟 p 交换的;

(3) G 的每个截断既对 p 阶元有拟 p 交换性又有唯一性基底;

(4) G 是 P_2 群且每个截断有唯一性基底.

证明 由 [151] 中的命题 19 得 (1) $\Rightarrow$ (2).

(2) $\Rightarrow$ (1). 与命题 14.1.5 相同, 设 G 是适合条件 (2) 的极小非 P 群. 注意拟 p 交换性蕴涵对 p 阶元有拟 p 交换性. 由命题 14.1.5 知, G 是 P_2 群, 从而 $\Omega_1(G)=\Omega_{\{1\}}(G)$. 又根据 [151] 中的定理 9 知, $G=\langle a,b\rangle$ 是二元生成的且 $\mho_1(G)$ 是 p 阶群. 特别地, 由 G 为 P_2 群可知, $\Omega_1(G)=\Phi(G)$ 成立. 于是 $a,b\notin\Omega_1(G)=\Omega_{\{1\}}(G)$. 故 a^p,b^p 一定都不是单位元. 又据 $|\mho_1(G)|=p$ 立得 $\langle a^p\rangle=\langle b^p\rangle$. 由 G 的拟 p 交换性知, 存在 i,j 使得 $(a^ib^j)^p$=1, 其中 $ij\not\equiv 0(\mathrm{mod}\ p)$. 这表示 $a^ib^j\in\Omega_1(G)=\Phi(G)$. 注意到 $j\not\equiv 0(\mathrm{mod}\ p)$ 就有 $G=\langle a,b\rangle=\langle a,a^ib^j\rangle=\langle a\rangle$. 矛盾.

由拟 p 交换性蕴涵对 p 阶元有拟 p 交换性以及 [151] 中的定理 23 得 (1) $\Rightarrow$ (3). 由命题 14.1.5 得 (3) $\Rightarrow$ (4).

(4) $\Rightarrow$ (1). 设 G 是适合条件 (4) 的极小非 P 群, 据 [151] 中的定理 9 知, $G=\langle a,b\rangle$ 是二元生成的, $\exp(G)=p^2$, 且 $\mho_1(G)$ 是 p 阶群. 特别地, 由 G 为 P_2 群得 $\Omega_1(G)=\Phi(G)$.

设 $\{a_1,a_2,\cdots,a_r\}$ 是 G 的一组唯一性基底, a_i 的阶为 p^{μ_i}. 则必有 $\mu_i=1$ 或 2, $i=1,2,\cdots,r$. 令交换 p 群 $H=\langle b_1\rangle\times\langle b_2\rangle\times\cdots\times\langle b_r\rangle$, 其中 $o(b_i)=p^{\mu_i}$, $i=1,2,\cdots,r$. 考虑从 G 到 H 的映射

$$f:\ a_1^{n_1}a_2^{n_2}\cdots a_r^{n_r}\mapsto b_1^{n_1}b_2^{n_2}\cdots b_r^{n_r}.$$

由唯一性基底的定义及 H 的构造可知, f 必是 G 到 H 上的一一映射. $\mho_1(H)$ 的元素形如 $b_1^{n_1p}b_2^{n_2p}\cdots b_r^{n_rp}$, 它在 G 中的原像为 $a_1^{n_1p}a_2^{n_2p}\cdots a_r^{n_rp}$, 且属于 $\mho_1(G)$. 于是

$$1\leqslant|\mho_1(H)|\leqslant|\mho_1(G)|=p.$$

也就有 $|\mho_1(H)|=1$ 或 p. 这表明或者

(i) $\mu_1=\mu_2=\cdots=\mu_r=1$,

或者

(ii) $\mu_1,\mu_2,\cdots,\mu_r$ 中只有一个为 2 其余皆为 1. 比如, $\mu_j=2$.

对于 (i), $G=\Omega_1(G)$ 成立. 这与 $\Omega_1(G)=\Phi(G)$ 矛盾. 对于 (ii), $|G|=p^{r+1}$. 再由 $|G:\Phi(G)|=p^2$ 知, $|\Phi(G)|=p^{r-1}$, 即 $|\Omega_1(G)|=p^{r-1}$. 但是, 注意到

$a_1, \cdots, a_{j-1}, a_j^p, a_{j+1}, \cdots, a_r$ 都是 p 阶元, 则集合

$$\{a_1^{n_1} \cdots a_{j-1}^{n_{j-1}} a_j^{pn_j} a_{j+1}^{n_{j+1}} \cdots a_r^{n_r} \mid 0 \leqslant n_i < p, i = 1, 2, \cdots, r\}$$

的不同元素共计 p^r 个且皆属于 $\Omega_1(G)$, 即 $|\Omega_1(G)| \geqslant p^r$. 矛盾. □

注 下面例 14.1.10 的 $\overline{G}$ 表明, 每个截断都有唯一性基的群不一定是 P 群. 该例还表明, 条件 (4) 作为 P 群的充分条件时, G 是 P_2 群, 不能减弱为 G 是 P_1 群.

定理 14.1.7 设 G 是有限 p 群. 则下列陈述等价.

(1) G 是正则 p 群;

(2) G 是 P 群且每个断对 p 阶元有 p 交换性;

(3) G 的每个截断既对 p 阶元有 p 交换性又有唯一性基底;

(4) G 的每个截断既有拟 p 交换性又对 p 阶元有 p 交换性;

(5) G 的每个截断是半 p 交换的.

证明 由正则群的性质及 [151] 中的定理 23 可知, (1) $\Rightarrow$ (2) $\Rightarrow$ (3). 由定理 14.1.6 有 (2) $\Leftrightarrow$ (4). 又由正则群的性质以及半 p 交换性蕴涵拟 p 交换性、对 p 阶元有 p 交换性, 有 (1) $\Rightarrow$ (5) $\Rightarrow$ (4). 只要再证 (3) $\Rightarrow$ (1) 即可.

设 G 是适合条件 (3) 的极小非正则群且 $\exp G = p^e$, 而 a 是一个 p^e 阶元. 据 [149] 中的定理 2 知, $\exp G' = p$ 且 $\mho_1(G)$ 是 p^{e-1} 阶循环群. 特别地, 当 $e > 2$ 时, 还有 $\Omega_1(G) = \Omega_{\{1\}}(G)$ 且 $G/\Omega_1(G) \cong \mho_1(G)$. 下面分两种情况证明 G 是 p 交换的, 从而是正则 p 群. 矛盾, 这就完成了证明.

当 $e > 2$ 时, $G/\Omega_1(G)$ 也是 p^{e-1} 阶循环群, 特别地, $G/\Omega_1(G) = \langle a\Omega_1(G)\rangle$. 因此, G 的任意两个元素 x 和 y 可分别表示为 $a^i s$ 和 $a^j t$, 其中 $s, t \in \Omega_1(G) = \Omega_{\{1\}}(G)$, 即 $s^p = t^p = 1$. 于是, 利用 G 对 p 阶元有 p 交换性, 并注意 $\exp(G') = p$, 就有

$$(xy)^p = (a^i s \cdot a^j t) = (a^i a^j [s, a^j] t)^p = ((a^i a^j)^p) = a^{ip} a^{jp} = (a^i s)^p (a^j t)^p = x^p y^p,$$

这表明 G 是 p 交换的.

当 $e \leqslant 2$ 时, 若 $e = 1$, 显然 G 是 p 交换的. 下面考虑 $e = 2$. 用与定理 14.1.6 的相同方法和记号, 也有 (i) 或 (ii) 成立. 设

$$x = a_1^{m_1} a_2^{m_2} \cdots a_r^{m_r}, \quad y = a_1^{n_1} a_2^{n_2} \cdots a_r^{n_r}$$

是 G 的任意两个元素. 对于 (i), 反复利用 G 对 p 阶元有 p 交换性, 立得 $x^p = 1$. 故 G 必是 p 交换的. 对于 (ii), 与 $e > 2$ 时类似, 但注意唯有 a_j 为 p^2 阶元, 我们也有

$$\begin{aligned}(xy)^p &= (a_1^{m_1} \cdots a_{j-1}^{m_{j-1}} a_j^{m_j} a_{j+1}^{m_{j+1}} \cdots a_r^{m_r} \cdot a_1^{n_1} \cdots a_{j-1}^{n_{j-1}} a_j^{n_j} a_{j+1}^{n_{j+1}} \cdots a_r^{n_r})^p \\ &= (a_j^{m_j} a_{j+1}^{m_{j+1}} \cdots a_r^{m_r} \cdot a_1^{n_1} \cdots a_{j-1}^{n_{j-1}} a_j^{n_j})^p\end{aligned}$$

$$= (a_j^{m_j} a_j^{n_j} a_{j+1}^{m_{j+1}} \cdots a_r^{m_r} \cdot a_1^{n_1} \cdots a_{j-1}^{n_{j-1}} c)^p = a_j^{m_j p} a_j^{n_j p}$$
$$= (a_1^{m_1} \cdots a_{j-1}^{m_{j-1}} a_j^{m_j} a_{j+1}^{m_{j+1}} \cdots a_r^{m_r})^p (a_1^{n_1} \cdots a_{j-1}^{n_{j-1}} a_j^{n_j} a_{j+1}^{n_{j+1}} \cdots a_r^{n_r})^p$$
$$= x^p y^p,$$

其中 $c = [a_{j+1}^{m_{j+1}} \cdots a_r^{m_r} \cdot a_1^{n_1} \cdots a_{j-1}^{n_{j-1}}, a_j^{n_j}] \in G'$, 这表明 G 是 p 交换的. □

注 例 14.1.9 表明, 条件 (2) 作为正则 p 群的充分条件时, G 是 P 群不能减弱为 G 是 P_2 群.

最后, 我们给出上面提到的几个例子, 需要用到换位子的如下公式.

设 G 是亚交换 p 群, $a, b, c \in G, d \in G'$, 则

$$\begin{gathered}[a,b] = [b,a]^{-1}, \quad [ab,c] = [a,c][a,c,b][b,c], \\ [a,bc] = [a,c][a,b][a,b,c], \quad [ad,b] = [a,b][d,b], [d^{-1},a] = [d,a]^{-1}.\end{gathered} \tag{14.1}$$

又若 $\exp(G') = p$, 则

$$(ab^{-1})^p = a^p \prod_{i=1}^{p-1} [ia, (p-i)b] b^{-p}, \tag{14.2}$$

若 $c(G) = p$, $a_1, a_2, \cdots, a_p \in G$, $i_1, i_2, \cdots, i_p$ 为整数, 则

$$[a_1^{i_1}, a_2^{i_2}, \cdots, a_p^{i_p}] = [a_1, a_2, \cdots, a_p]^{i_1 i_2 \cdots i_p}. \tag{14.3}$$

以下不加声明时, 同余式皆是模 3 的.

例 14.1.8 设

$$G_1 = \langle a, b \mid a^9 = b^9 = c^3 = 1, [a,b] = c, [a,c] = b^3, [b, c = 1], [a^3, b] = [b^3, a] = 1 \rangle;$$

$$G_2 = \langle x, y \mid x^9 = y^9 = z^9 = 1, [x,y] = z, [x,z] = [y,z] = 1 \rangle.$$

令 $G = G_1 \times G_2, H = \langle ax, by \rangle$. 则 G 是拟 p 交换的, 但是 H 不是 P_1 群. 从而 G 不是 P_1 群. 由此还知, G 对 p 阶元有拟 p 交换性, 但不是 P_2 群.

证明 容易验证, G_1 是 3^5 阶亚交换群, 且 $\exp(G_1) = 9, \exp(G_1') = 3, c(G_1) = 3, \mho_1(G_1) = Z(G_1)$, 它的元素均可表示成 $a^i b^j c^k$ 的形状, 其中 i, j 模 9, k 模 3 唯一确定; G_2 是 3^6 阶亚交换群, 且 $\exp(G_2) = 9, c(G_2) = 2$(从而 G_2 是正则的), 它的元素均可表示成 $x^i y^j z^k$ 的形状, 其中 i, j, k 模 9 唯一确定.

先证 G 是拟 p 交换的. 设

$$gu, hv \in G, \quad \text{其中 } g = a^i b^j c^k, \quad h = a^m b^n c^l \in G_1, \quad u, v \in G_2.$$

用公式 (14.1)—(14.3), 并注意 $c(G_1) = 3$, 就有

$$[g,h,g] = [a,b,a]^{ni^2} [a,b,b]^{nij} [b,a,a]^{mij} [b,a,b]^{mj^2} = [c,a]^{ni^2} [c^{-1},a]^{mij} = b^{3(mij - ni^2)},$$

$$[g,h,h]=[a,b,a]^{mni}[a,b,b]^{n^2i}[b,a,a]^{m^2j}[b,a,b]^{mnj}=[c,a]^{mni}[c^{-1},a]^{m^2j}=b^{3(m^2j-mni)}.$$

于是, 用 (14.2), (14.3) 及 $\mho_1(G_1)=Z(G_1)$ 得

$$(g^\alpha h^{-\beta})^3=g^{3\alpha}h^{-3\beta}[g,h,g]^{\alpha^2\beta}[g,h,h]^{\alpha\beta^2}=g^{3\alpha}h^{-3\beta}b^{3(mij-ni^2)\alpha^2\beta+3(m^2j-mni)\alpha\beta^2}. \tag{14.4}$$

同样有

$$(a^sb^tc^r)^3=a^{3s}b^{3(t+s^2t)}=\begin{cases} b^{3t}, & s\equiv 0,\\ a^{3s}b^{-3t}, & s\not\equiv 0.\end{cases} \tag{14.5}$$

再注意 G_2 是正则的, 则 $(u^\alpha v^{-\beta})^3=1 \Longleftrightarrow u^{3\alpha}=v^{3\beta}$. 因此

$$\langle (gu)^3\rangle=\langle (hv)^3\rangle \Longleftrightarrow (gu)^3=(hv)^{3t}\Longleftrightarrow \begin{cases} g^3=h^{3t}, & (14.6)\\ u^3=v^{3t}, & (14.7)\end{cases}$$

其中 $t\not\equiv 0$;

$$((gu)^\alpha(hv)^{-\beta})^3=1\Longleftrightarrow \begin{cases}(g^\alpha h^{-\beta})^3=1\\ (u^\alpha v^{-\beta})^3=1\end{cases}\Longleftrightarrow \begin{cases}(g^\alpha h^{-\beta})^3=1, & (14.8)\\ u^{3\alpha}=v^{3\beta}. & (14.9)\end{cases}$$

分下面两种情况讨论.

(i) $mi\equiv 0$. 不妨设 $i\equiv 0$, 这时由 (14.5) 有

$$g^3=b^{3i}. \tag{14.10}$$

代入 (14.4), 并注意 $\exp(G_1)=9$, 得

$$(g^\alpha h^{-\beta})^3=h^{-3\beta}b^{3(1+m^2\beta^2)j\alpha}. \tag{14.11}$$

若存在 $\alpha,\beta,\alpha\beta\not\equiv 0$ 使得 $((gu)^\alpha(hv)^{-\beta})^3=1$, 则由 (14.8) 和 (14.10), 并用 $\gamma^2\equiv 1$(当 $\gamma\not\equiv 0$ 时), 得 $h^3=b^{3(1+m^2)j\alpha\beta}$. 与 (14.5) 比较, 必有 $m\equiv 0$ 且 $h^3=b^{3n}$. 于是, 由 $b^{3n}=b^{3(1+m^2)j\alpha\beta}=b^{3j\alpha\beta}$ 得 $n=j\alpha\beta$. 注意 $\alpha\beta\not\equiv 0$. 也就有 $j\equiv n\alpha\beta$. 由 (8) 有 $g^3=b^{3j}=b^{3n\alpha\beta}=h^{3\alpha\beta}$. 又由 (14.9) 有 $u^{3\alpha}=v^{3\beta}$. 注意 $\exp G_2=9$, 即 $u^3=v^{3\alpha\beta}$. 据 (14.6) 和 (14.7) 知得 $\langle (gu)^3\rangle=\langle (hv)^3\rangle$ 成立.

反之, 若 $\langle (gu)^3\rangle=\langle (hv)^3\rangle$, 由 (14.6) 和 (14.10) 得 $h^{3t}=b^{3j}(t\not\equiv 0)$, 从而 $h^3=b^{3jt}$. 当 $j\equiv 0$ 时有 $h^3=1$. 取 $\alpha=1,\beta=t$. 则 $\alpha\beta\not\equiv 0$. 且由 (9) 得 $(g^\alpha h^{-3\beta})^3=1$. 又由 (14.7) 得 $u^3=v^{3t}$, 即 $u^{3\alpha}=v^{3\beta}$. 据 (14.8) 和 (14.9) 知, $((gu)^\alpha(hv)^{-\beta})^3=1$ 成立. 当 $j\not\equiv 0$ 时, 将 $h^3=b^{3jt}$ 与 (14.5) 比较, 必有 $m\equiv 0$ 且 $h^3=b^{3n}$. 于是, 由 $b^{3n}=b^{3jt}$ 得 $n\equiv jt$. 特别地, $n\not\equiv 0$. 这时取 $\alpha=j,\beta=n$. 则 $\alpha\beta\not\equiv 0$, 且由 (14.11) 得

$$(g^\alpha h^{-\beta})^3=h^{-3n}b^{3j^2}=b^{-3n^2}b^{3j^2}=b^{-3}b^3=1.$$

又由 (14.7) 得 $u^3 = v^{3t}$. 从而 $u^{3\alpha} = v^{3t\alpha} = v^{3tj} = v^{3n} = v^{3\beta}$. 据 (14.8) 和 (14.9) 知, $((gu)^{\alpha}(hv)^{-\beta})^3 = 1$ 成立.

(ii) $mi \not\equiv 0$. 与 (i) 类似, 细节略.

综上所述, G 是拟 p 交换的. 下面证 H 不是 P_1 群.

记 $u = ax, v = by$, 则 $w = [u, v] = cz$, $[u, w] = b^3, [v, w] = 1$. 注意 G 是亚交换群且 $c(G) = 3$. 据命题 1.1.9, 有

$$[u^s, v^t] = \prod_{i=1}^{s}\prod_{j=1}^{t}[iu, jv]^{\binom{s}{i}\binom{t}{j}}.$$

经整理, $[u^s, v^t]$ 形如 $w^k b^{3l}$. 由此不难验证, H 的元素均可表示成 $u^m v^n w^k b^{3l}$ 的形状, 且 m, n, k 模 9, l 模 3 唯一确定.

我们来计算 $\mho_{\{1\}}(H)$. 为方便, 记 H 的任意元素为 $u^m v^{-n} w^k b^{3l}$, 其中 m, n, k, l 皆为非负整数. 由 $c(G_2) = 2$, 用命题 1.1.9 和命题 1.1.10, 有

$$\begin{aligned}(x^m y^{-n} z^k)^3 &= (x^m y^{-n})^3 z^{3k} = x^{3m} \prod_{i+j\leqslant 3}[ix^m, jy^n]^{\binom{3}{i+j}} y^{-3n} z^{3k} \\ &= x^{3m}[x^m, y^n]^3 y^{-3n} z^{3k} = x^{3m}\prod_{i=1}^{m}\prod_{j=1}^{n}[ix, jy]^{3\binom{m}{i}\binom{n}{j}} y^{-3n} z^{3k} \\ &= x^{3m}[x, y]^{3mn} y^{-3n} z^{3k} = x^{3m} y^{-3n} z^{3(k+mn)}.\end{aligned}$$

(显然, 对 $m = 0$ 或 $n = 0$, 上式也成立). 再利用 (14.5), 就有

$$\begin{aligned}(u^m v^n w^k b^{3l})^3 &= (a^m b^{-n} c^k)^3 (x^m y^{-n} z^k)^3 = a^{3m} b^{-3(n+m^2 n)} x^{3m} y^{-3n} z^{3(k+mn)} \\ &= u^{3m} v^{-3n} w^{3(k+mn)} b^{-3m^2 n}.\end{aligned} \tag{14.12}$$

取 $m = 1, n = 8, k = 1, l = 0$, 即可知 $u^3 v^3 b^3 \in \mho_{\{1\}}(H)$. 又, $v^3 \in \mho_{\{1\}}(H)$. 我们断定 $u^3 v^3 b^3 \cdot v^3 = u^3 v^6 b^3 \notin \mho_{\{1\}}(H)$. 若不然, 必存在 $u^m v^n w^k b^{3l} \in H$ 使得 $(u^m v^n w^k b^{3l})^3 = u^3 v^6 b^3$. 由 (14.12) 即有

$$u^{3m} v^{-3n} w^{3(k+mn)} b^{-3m^2 n} = u^3 v^6 b^3.$$

于是 $3m \equiv 3 (\mathrm{mod}\ 9)$, $-3n \equiv 6 (\mathrm{mod}\ 9)$, $-m^2 n \equiv 1 (\mathrm{mod}\ 3)$, 这就引出 $1 \equiv -1 (\mathrm{mod}\ 3)$ 的矛盾. 这些表明, $\mho_{\{1\}}(H) \neq \mho_1(H)$, 即 H 不是 P_1 群. □

例 14.1.9 设 $G = \langle a, b \mid a^9 = 1, b^3 = a^{-3}, [a, b] = c, c^3 = 1, [a, c] = a^3, [b, c] = 1\rangle$. 易知, G 是 P_2 群且为极小非 P 群 ([238] 中的定理 11 的 J_3). 不难验证, G 的每个截断对 p 阶元有 p 交换性.

例 14.1.10 设 $G=\langle a,b \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=a^{-3},[b,c=1],[a^3,b]=[b^3,a]=1\rangle$. 则 G 是极小非 P_1 群 ([238] 中的定理 10 的 I_3). 可以验证, G 对 p 阶元有 p 交换性. 然而 $\overline{G}=G/\langle b^3\rangle$ 对 p 阶元没有 p 交换性. 事实上,

$$\overline{G}=\langle \bar{a},\bar{b} \mid \bar{a}^9=\bar{b}^3=\bar{c}^3=\bar{1},[\bar{a},\bar{b}]=\bar{c},[\bar{a},\bar{c}]=\bar{a}^3,[\bar{b},\bar{c}]=\bar{1}\rangle.$$

但是, 这组关系定义了一个 3^4 阶极小非 P_2 群 ([238] 中的定理 11 的 J_2). 由 $|\overline{G}|=3^4$, 这组关系即为 $\overline{G}$ 的定义关系, 故 $\overline{G}$ 为极小非 P_2 群. 据 [151] 中的定理 6, 存在 $\bar{u},\bar{v}\in\overline{G}$, 使 $\overline{G}=\langle\bar{u},\bar{v}\rangle$, 而 $\bar{u}^3=\bar{v}^3=\bar{1}$, 但 $(\bar{u}\bar{v})^3\neq\bar{1}$. 又, 易知 $\overline{G}$ 的每个截断都有唯一性基底, 由 [151] 中的定理 6 知, $\overline{G}$ 是 P_1 群.

下面介绍 p^{p+1} 阶亚交换的非正则 p 群的幂结构及有关结果. 以下用 $\mathcal{P}_i$ 表示 P_i 群类.

命题 14.1.11 设 G 是 p^{p+1} 阶群. 则 G 是非正则群当且仅当 G 是极大类 p 群.

对 $p>3$, 这个命题是 [89] 中的III, 定理 10.11 和定理 14.21 的直接推论. 对 $p=2,3$, 可见命题 14.1.12 和命题 14.1.13. 于是, 我们所考察的问题等价地就是考察 p^{p+1} 阶亚交换的极大类 p 群的幂结构.

我们先处理 $p=2$ 和 3 的情况.

命题 14.1.12 8 阶非正则群只有二面体群 D_8 和四元数群 Q_8, 它们都是亚交换的极大类 2 群, 且 $\mathrm{D}_8\in\mathcal{P}_1\backslash\mathcal{P}_2$, $\mathrm{Q}_8\in\mathcal{P}_2\backslash\mathcal{P}_3$.

命题 14.1.13 3^4 阶非正则群都是亚交换的极大类 3 群. 反之亦然; 它们都包含交换的极大子群, 共有四种类型, 即

(1) $G=\langle a,b \mid a^9=b^3=c^3=1,\ [a,b]=c,\ [a,c]=1,\ [b,c]=a^3\rangle$;

(2) $G=\langle a,b \mid a^9=b^3=c^3=1,\ [a,b]=c,\ [a,c]=a^3,\ [b,c]=1\rangle$;

(3) $G=\langle a,b \mid a^9=1,b^3=a^{-3},c^3=1,\ [a,b]=c,\ [a,c]=a^3,\ [b,c]=1\rangle$;

(4) $G=\langle a,b \mid a^9=1,b^3=a^3,c^3=1,\ [a,b]=c,\ [a,c]=a^3,\ [b,c]=1\rangle$, 且 (1), (2) 型群属于 $\mathcal{P}_1\backslash\mathcal{P}_2$, (3) 型群属于 $\mathcal{P}_2\backslash\mathcal{P}_3$, (4) 型群属于 $\mathcal{P}_3$.

命题 14.1.13 的证明, 见 [238] 中的定理 11. 从现在起, 无特别声明, 总设素数 $p>3$.

由 [89] 中的III, 定理 14.11 即得如下引理.

引理 14.1.14 p^{p+1} 阶的亚交换的极大类 p 群是非例外群.

引理 14.1.15 设 G 是 p^{p+1} 阶的亚交换的极大类 p 群. 则

(1) $G'=\Phi(G)$ 是 p^{p-1} 阶初等交换群;

(2) $\exp(G)=p^2$;

(3) $G_p=Z(G)=\mho_1(G)=\mho_{\{1\}}(G)$ 是 p 阶群.

证明 只需证 $\mho_1(G)=\mho_{\{1\}}(G)$. 其他结论都是 [89] 中的III, 引理 10.11, 引理 14.2 和引理 14.14 的直接推论. 既然, $\exp(G)=p^2$, 就可取到 G 的 p^2 阶元素 a. 再注意到 $|\mho_1(G)|=p$. 则有 $\mho_1(G)=\langle a^p\rangle$. 从而 $\mho_1(G)=\mho_{\{1\}}(G)$. □

定理 14.1.16 设 G 是 p^{p+1} 阶的亚交换的非正则群, 则

(1) $G\in\mathcal{P}_1$;

(2) $G\in\mathcal{P}_1\backslash\mathcal{P}_2$ 当且仅当 $G=\Omega_1(G)$;

(3) $G\in\mathcal{P}_2\backslash\mathcal{P}_3$ 当且仅当 $|G:\Omega_1(G)|=p^2$;

(4) $G\in\mathcal{P}_3$ 当且仅当 $|G:\Omega_1(G)|=p$.

证明 G 的每个真截断的阶 $\leqslant p^p$, 故它们都是正则群. 从而有性质 $P_i(i=1,2,3)$. 因此, 为证 G 是 P_i 群, 只要证 G 本身有性质 P_i. 又注意到 $\exp(G)=p^2$, P_i 中的等式对 $n=2$ 恒成立, 故只需再考虑 $n=1$. 由引理 14.1.15(3), $G\in\mathcal{P}_1$ 成立. 由 $|\mho_1(G)|=p$, 结论 (4) 成立. 设 $G\in\mathcal{P}_2\backslash\mathcal{P}_3$, 则 $\Omega_1(G)=\Omega_{\{1\}}(G)$. 然而, $\exp(G)=p^2$ 且 $\exp(G')=p$, 故 $G'\leqslant\Omega_1(G)=\Omega_{\{1\}}(G)\not\leqslant G$. 由 $G\in\mathcal{P}_3$ 及前面的说明知, $|G:\Omega_1(G)|\neq|\mho_1(G)|=p$. 于是, 必有 $|G:\Omega_1(G)|=p^2$. 反之, 若 $|G:\Omega_1(G)|=p^2$, 显然, $G\notin\mathcal{P}_3$. 又 $G'\subseteq\Omega_{\{1\}}(G)\subseteq\Omega_1(G)$ 且 $|G:G'|=p^2$, 故 $\Omega_1(G)=\Omega_{\{1\}}(G)$. 从而 $G\in\mathcal{P}_2$. 这样 (3) 成立. 由 (1), (3) 和 (4) 知, (2) 成立. □

下面将用定义关系描述 p^{p+1} 阶的亚交换的非正则群的幂结构.

引理 14.1.17 设 G 是 p^{p+1} 阶 $(p>3)$ 亚交换的极大类 p 群. 则

(1) $G=\langle x,y\rangle$, $[y,x]=u_2$, $[u_i,x]=u_{i+1}(i=2,\cdots,p-1)$, $[u_p,x]=1$, $[u_2,y]=u_k^{a_k}\cdots u_p^{a_p}$, $[u_i,u_j]=1(i\neq j)$, $u_i^p=1$, $x^p=u_p^w$, $y^p=u_p^{z-1}$, 其中, 参数 $a_k\not\equiv 0(\mathrm{mod}\ p)$ 而 $k\geqslant 4$, 或者 $a_k\equiv\cdots\equiv a_p\equiv 0(\mathrm{mod}\ p)$, $(w,z)=(0,0)$ 或者 $(1,z)$, z 为任意整数;

(2) G 的任意元素都可表示成 $x^my^n\prod\limits_{i=2}^{p}u_i^{s_i}$ 的形式, 其中 $m,n,s_i(i\geqslant 2)$ 都是模 p 唯一确定的, 且下面的等式成立

$$\left(x^my^n\prod_{i=2}^{p}u_i^{s_i}\right)^p=(x^my^n)^p=u_p^{mw+n(z-1)+m^{p-1}n}. \tag{14.13}$$

证明 (1) 由引理 14.1.14 知, G 是非例外群. 再由 [89] 中的III, 引理 14.8 知, 存在 G 的生成元集合 $\{x,y\}$ 使得 $G_1=\langle G_2,y\rangle$ 且

$$[y,x]=u_2,\quad [u_i,x]=u_{i+1}(i=2,\cdots,p-1),\quad G_i=\langle G_{i+1},u_i\rangle(i=2,\cdots,p).$$

于是由 $G_{p+1}=1$ 得 $G_i=\langle u_i,\cdots,u_p\rangle$. 特别地, 对 $i=2$, 注意到 G_2 是 p^{p-1} 阶的初等交换群. 则 $\{u_2,\cdots,u_p\}$ 必为 G_2 的一组基. 对 $i=p$, 有 $G_p=\langle u_p\rangle$. 用引理 14.1.15(3) 得 $[u_p,x]=1$. 依非例外群的定义, $[u_2,y]\in[G_2,G_1]\leqslant G_4$. 故 $[u_2,y]=u_k^{a_k}\cdots u_p^{a_p}$, 且在 G_1 为非交换群时, $a_k\not\equiv 0(\mathrm{mod}\ p)$, 而 $k\geqslant 4$. 在 G_1 为交

换群时, $a_k \equiv \cdots \equiv a_p \equiv 0 (\mathrm{mod}\ p)$. 引理 14.1.15(3) 表明 $x^p, y^p \in G_p$. 故 $x^p = u_p^w$, $y^p = u_p^{z-1}$. 反之, 利用循环扩张的理论可知, 这组关系定义了一个 p^{p+1} 阶的亚交换的极大类 p 群 (细节略). 证明了 (2) 之后, 我们再讨论 (w, z).

(2) 先证一个等式, 即当 $2 \leqslant j \leqslant p-1$ 时, 有

$$[jy, (p-j)x] = 1.$$

这是因为 G 是非例外群, 故 $[G_i, y] \leqslant [G_i, G_1] \leqslant G_{i+2}$. 对 j 作归纳法易知, 当 $2 \leqslant j \leqslant p-1$ 时, $[u_{p-j+1}, (j-1)y] = 1$. 于是

$$[jy, (p-j)x] = [[[y, x], (p-j-1)x], (j-1)y] = [u_{p-j+1}, (j-1)y] = 1.$$

因 $d(G/\Phi(G)) = 2$ 而 $\Phi(G) = G_2$ 为初等交换群, 故 G 的元素都可以表成 $x^m y^n \prod\limits_{i=2}^{p} u_i^{s_i}$ 的形式, 其中 $m, n, s_i (i \geqslant 2)$ 模 p 唯一确定. 记 $d = \prod\limits_{i=2}^{p} u_i^{s_i}$, 则由亚交换群的计算公式 (即徐公式) 及上述证得的等式可得

$$\begin{aligned}(x^m y^n d)^p &= (x^m y^n)^p = x^{mp} y^{np} \prod_{i+j=p} [ix, jy]^{m^i (-n)^j} \\ &= x^{mp} y^{np} \prod_{i+j=p} [jy, ix]^{-m^i (-n)^j} = x^{mp} y^{np} [y, (p-1)x]^{-m^{p-1}(-n)} \\ &= u_p^{mw + n(z-1) + m^{p-1} n}.\end{aligned}$$

最后讨论 (w, z). 在 $w \not\equiv 0 (\mathrm{mod}\ p)$ 时, 令 $x' = x^{w^{-1}}$, $y' = y$, 这里 $w^{-1} w \equiv 1 (\mathrm{mod}\ p)$. 于是 $G = \langle x', y' \rangle$ 且 $G_1 = \langle G_2, y' \rangle$. 记

$$[y', x'] = u'_2, \quad [u'_i, x'] = u'_{i+1} \quad (2 \leqslant i \leqslant p-1).$$

则 $u'_p \in G_p$. 由引理 14.1.15(3) 就有 $[u'_p, x'] = 1$. 仍然有

$$[u'_2, y'] = u_l^{b_l} \cdots u_p^{b_p}, \quad [u'_i, u'_j] = 1 (i \neq j), \quad u_i'^p = 1,$$

且若 $b_l \not\equiv 0 (\mathrm{mod}\ p)$, 则还有 $l \geqslant 4$(事实上, $l = k$ 是群 G 的不变量, 可见 [159]). 又, 用 $w^{p-1} \equiv 1 (\mathrm{mod}\ p)$ 及公式

$$[a_1^{i_1}, \cdots, a_p^{i_p}] = [a_1, \cdots, a_p]^{i_1 \cdots i_p}$$

可得

$$u'_p = [y', (p-1)x'] = [y, (p-1)x^{w^{-1}}] = [y, (p-1)x]^{w^{-(p-1)}} = [y, (p-1)x] = u_p.$$

于是

$$(x')^p = x^{pw^{-1}} = u_p^{ww^{-1}} = u_p = u'_p, \quad (y')^p = y^p = u_p^{z-1} = (u'_p)^{z-1}.$$

这表明, 此时总可归为 $(w,z)=(1,z)$, z 为任意. 在 $w\equiv 0$ 而 $z\not\equiv 0 \pmod p$ 时, 令 $x'=(xy)^{z^{-1}}, y'=y$, 类似地, 记 u'_i 同前述. 对 i 作归纳并注意到 $[u_i,y]\in G_{i+2}$, 易证当 $1\leqslant i\leqslant p-1$ 时, $[y,i(xy)]\equiv u_{i+1} \pmod{G_{i+2}}$. 注意到 $G_{p+1}=1$ 就有

$$u'_p=[y',(p-1)x']=[y,(p-1)(xy)]=u_p.$$

然后用 (2) 中的公式就有

$$(x')^p=(xy)^{pz^{-1}}=u_p=u'_p.$$

又 $(y')^p=y^p=u_p^{z-1}=(u'_p)^{z-1}$. 这表明, 第二种情况总可归为 $(w,z)=(1,z)$. 综合起来, 我们总可设 $(w,z)=(0,0)$ 或 $(1,z)$, z 为任意整数. □

定理 14.1.18　设 G 是 p^{p+1} 阶 $(p\geqslant 3)$ 的亚交换的非正则群. 则 G 如引理14.1.17(1)所设, 并且

(1) 当 $(w,z)=(0,0)$ 或 $(1,1)$ 时, 群不同构且 $G\in\mathcal{P}_1\backslash\mathcal{P}_2$;

(2) 当 $(w,z)=(1,0)$ 时, $G\in\mathcal{P}_2\backslash\mathcal{P}_3$;

(3) 当 $(w,z)=(1,z)$ 且 $z\not\equiv 0,1 \pmod p$ 时, $G\in\mathcal{P}_3$.

证明　对于 $p=3$, 在命题 14.1.13 中, 对 (1) 型群, 令

$$x=b,\quad y=a,\quad u_2=c,\quad u_3=a^{-3},\quad (w,z)=(0,0);$$

对 (2)—(4) 型群, 令

$$x=a,\quad y=b,\quad u_2=c^{-1},\quad u_3=a^3$$

及 (w,z) 分别为 $(1,1)$, $(1,0)$ 与 $(1,2)$. 则易知结论成立. 以下总设 $p>3$.

由命题 14.1.11 知 G 有引理 14.1.17(1) 的定义关系. 与定理 14.1.16 的证明相同, 只要对 G 本身和 $n=1$ 验证性质 P_i 中的等式即可. 记 $d=\prod\limits_{i=2}^{p}u_i^{s_i}$. 已证总有 $G\in\mathcal{P}_1$.

(1) 设 $(w,z)=(0,0)$. 由引理 14.1.17(2), 当 $m\equiv 0 \pmod p$ 时, $(x^my^nd)^p=u_p^{-n}=1$ 当且仅当 $n\equiv 0 \pmod p$; 当 $m\not\equiv 0 \pmod p$ 时, 注意 $m^{p-1}\equiv 1 \pmod p$, 则总有 $(x^my^nd)^p=1$. 于是

$$\Omega_{\{1\}}(G)=\left\{\prod_{i=2}^{p}u_i^{s_i}\text{或}x^my^n\prod_{i=2}^{p-1}u_i^{s_i}\ \middle|\ s_i,n\text{为任意的整数},m\not\equiv 0 \pmod p\right\}.$$

而

$$|\Omega_{\{1\}}(G)|=p^{p-1}+(p-1)p\cdot p^{p-1}=p^{p-1}(p^2-p+1)>p^p.$$

因此, $\Omega_1(G)=\langle\Omega_{\{1\}}(G)\rangle=G\neq\Omega_{\{1\}}(G)$, 故 $G\in\mathcal{P}_1\backslash\mathcal{P}_2$.

又设 $(w,z)=(1,1)$. 当 $m\equiv 0(\mathrm{mod}\ p)$ 时, 总有 $(x^my^nd)^p=1$; 当 $m\not\equiv 0(\mathrm{mod}\ p)$ 时, $(x^my^nd)^p=u_p^{m+n}=1$ 当且仅当 $n\equiv -m(\mathrm{mod}\ p)$. 于是,

$$\Omega_{\{1\}}(G)=\left\{y^n\prod_{i=2}^{p}u_i^{s_i}\text{或}x^my^{-m}\prod_{i=2}^{p}u_i^{s_i}\ \middle|\ s_i,n\text{为任意的整数},m\not\equiv 0(\mathrm{mod}\ p)\right\}.$$

而

$$|\Omega_{\{1\}}(G)|=p\cdot p^{p-1}+(p-1)p^{p-1}=2p^p-p^{p-1}>p^p.$$

同上知, $G\in\mathcal{P}_1\backslash\mathcal{P}_2$. 比较 $|\Omega_{\{1\}}(G)|$ 知, $(w,z)=(0,0)$ 或 $(1,1)$ 时, 群互不同构.

(2) 设 $(w,z)=(1,0)$. 当 $m\equiv 0(\mathrm{mod}\ p)$ 时, $(x^my^nd)^p=u_p^{-n}=1$ 当且仅当 $n\equiv 0(\mathrm{mod}\ p)$; 当 $m\not\equiv 0(\mathrm{mod}\ p)$ 时, 总有 $(x^my^nd)^p=u_p^m\neq 1$. 于是, $\Omega_{\{1\}}(G)=G'$, 也就有 $\Omega_1(G)=\Omega_{\{1\}}(G)=G'$, 故 $G\in\mathcal{P}_2$. 又, $|G:\Omega_1(G)|=p^2\neq|\mho_1(G)|$. 因此 $G\in\mathcal{P}_2\backslash\mathcal{P}_3$.

(3) 设 $(w,z)=(1,z)$ 而 $z\not\equiv 0,1(\mathrm{mod}\ p)$. 当 $m\equiv 0(\mathrm{mod}\ p)$ 时, $(x^my^nd)^p=u_p^{n(z-1)}=1$ 当且仅当 $n\equiv 0(\mathrm{mod}\ p)$; 当 $m\not\equiv 0(\mathrm{mod}\ p)$ 时, $(x^my^nd)^p=u_p^{m+nz}=1$ 当且仅当 $n=-mz^{-1}$. 于是

$$\Omega_{\{1\}}(G)=\left\{\prod_{i=2}^{p}u_i^{s_i}\text{或}x^my^{-mz^{-1}}\prod_{i=2}^{p}u_i^{s_i}\ \middle|\ s_i\text{为任意的整数},m\not\equiv 0(\mathrm{mod}\ p)\right\}.$$

而

$$|\Omega_{\{1\}}(G)|=p^{p-1}+(p-1)p^{p-1}=p^p.$$

不难知, $\Omega_{\{1\}}(G)$ 对乘法封闭, 故 $\Omega_1(G)=\Omega_{\{1\}}(G)$ 且为 p^p 阶. 又这时还有 $|G:\Omega_1(G)|=p=|\mho_1(G)|$. 因此, $G\in\mathcal{P}_3$. □

注 Miech 在 [159] 中给出了由 $\{a_k,\cdots,a_p;w,z\}$ 判断 G 是否同构的计算方法, 步骤很复杂. 定理 14.1.18 表明, 对于 p^{p+1} 阶的亚交换的非正则群, 它们的 $\mathcal{P}_i$ 性质与参数 $a_k,\cdots,a_p$ 无关, 只与 (w,z) 有关.

作为定理 14.1.18 的一个应用, 我们有如下推论.

推论 14.1.19 如果 p^{p+1} 阶 $(p\geqslant 3)$ 的亚交换的非正则群 G 包含交换的极大子群, 那么, 这样的群共有 $p+1$ 个不同构的类型, 其中, 有两类是 $\mathcal{P}_1$ 群不是 $\mathcal{P}_2$ 群, 一类是 $\mathcal{P}_2$ 群不是 $\mathcal{P}_3$ 群, $p-2$ 类是 $\mathcal{P}_3$ 群.

证明 由命题 14.1.13 知, 对于 $p=3$ 结论成立. 以下设 $p>3$. 设 G 包含交换的极大子群 M. 注意到 G 作为极大类 p 群必是非例外群, 依 [89] 中的III, 定理 14.22(a), G 的每个异于 G_1 的极大子群都是极大类 p 群. 从而, 类为 $p-1$. 又, 交换群的类为 1, 故必有 $M=G_1$. 这样, 在引理 14.1.17(1) 所给的定义关系中,

必有 $a_k \equiv \cdots \equiv a_p \equiv 0 \pmod p$. 由定理 14.1.18, 只要再证, 当 $(w,z)=(1,z)$ 且 $z \not\equiv 0,1 \pmod p$ 时, z 为群 G 的不变量即可. 事实上, 这时, $G \in \mathcal{P}_3$ 且

$$\Omega_1(G)=\Omega_{\{1\}}(G)=\left\{\prod_{i=2}^{p} u_i^{s_i}\text{或}x^m y^{-mz^{-1}}\prod_{i=2}^{p-1} u_i^{s_i}\,\middle|\, s_i\text{为任意的整数}, m\not\equiv 0 \pmod p\right\}$$

为 p^p 阶群, 故 $\Omega_1(G)=\langle G_2, xy^{-z^{-1}}\rangle$. 今假设另有群 $H=\langle a,b\rangle$ 也满足定义关系

$$[b,a]=v_2,\quad [v_i,a]=v_{i+1}\ (i=2,\cdots,p-1),\quad [v_p,a]=1,$$

$$[v_2,b]=1,\quad [v_i,v_j]=1\ (i\neq j),\quad v_i^p=1,\quad a^p=v_p,\quad b^p=v_p^{c-1}.$$

我们来证明, 若存在从 G 到 H 的同构映射 σ, 则 $c\equiv z \pmod p$. 首先, 由引理 14.1.17 和定理 14.1.18 的证明可知, 对 H 同样有 $H_1=\langle H_2,b\rangle$, $\Omega_1(H)=\langle H_2, ab^{-c^{-1}}\rangle$, 这里, $H_i=K_i(G)(i=2,\cdots,p+1)$ 为 H 的下中心群列的项, 而 $H_1=C_H(H_2/H_4)$. 显然,

$$(xy^{-z^{-1}})^\sigma \in \Omega_1(G)^\sigma=\Omega_1(H),\quad y^\sigma\in G_1^\sigma=H_1.$$

因为 $H_2=\Phi(H)$ 及 $H/\Phi(H)$ 都为初等交换群, 故

$$(xy^{-z^{-1}})^\sigma \equiv (ab^{-c^{-1}})^m \equiv a^m b^{-mc^{-1}},\quad y^\sigma\equiv b^s (\mathrm{mod}\ \Phi(H)),$$

其中, $m,s\not\equiv 0 \pmod p$. 于是, $x^\sigma=a^m b^{sz^{-1}-mc^{-1}}d_1$, $y^\sigma=b^s d_2$, 其中 $d_1,d_2\in\Phi(H)$. 由 $m\neq 0, m^{p-1}\equiv 1 \pmod p$, H_1, H_2 交换及命题 1.1.9 有

$$\begin{aligned}u_p^\sigma&=[y,(p-1)x]^\sigma=[y^\sigma,(p-1)x^\sigma]=[b^s d_2,(p-1)(a^m b^{sz^{-1}-mc^{-1}}d_1)]\\&=[b^s,(p-1)(a^m b^{sz^{-1}-mc^{-1}})]=[b^s,(p-1)a^m]=[b,(p-1)a]^s=v_p^s.\end{aligned}$$

由 $y^p=u_p^{z-1}$, 有 $(y^\sigma)^p=(u_p^\sigma)^{z-1}$, 也就有 $(bd_2)^p=(v_p^s)^{z-1}$. 用引理 14.1.17(2), 有 $(b^s d_2)^p=b^{sp}=v_p^{s(c-1)}$. 于是 $s(z-1)\equiv s(c-1) \pmod p$. 由 $s\not\equiv 0 \pmod p$ 得 $c\equiv z \pmod p$. □

14.2 NC 群与拟 NC 群

众所周知, N/C 定理在有限群的研究中起着极其重要的作用. 基于此观察, Deaconescu 等在文献 [56] 引进一个新的概念: 设 G 是有限群, H 是 G 的子群. $\mathrm{Aut}_G(H):=N_G(H)/C_G(H)$ 被称为 H 在 G 中的**自同构导子**(automizer). 明显地, $\mathrm{Inn}(H)\leqslant \mathrm{Aut}_G(H)\leqslant \mathrm{Aut}(H)$. 在文献 [56] 中, 他们称 $\mathrm{Aut}_G(H)$ 是小的, 若 $\mathrm{Aut}_G(H)=\mathrm{Inn}(H)$; 称 $\mathrm{Aut}_G(H)$ 是大的, 若 $\mathrm{Aut}_G(H)=\mathrm{Aut}(H)$.

Zassenhaus [252] 的一个经典结果是: 有限群 G 是交换的当且仅当对 G 的所有交换子群 A 均有 $N_G(A) = C_G(A)$, 以自同构导子的术语, 即 G 的所有交换子群的自同构导子是小的. 近年来, 对自同构导子的研究比较活跃. 例如, Miyamoto 在文献 [162] 证明: 若有限群 G 的所有交换子群的自同构导子是大的, 则 G 是可解的. Burnside 的一个经典结果断言: 若有限群 G 的一个交换 Sylow 子群的自同构导子是小的, 则 G 是 p 幂零的. Lennox 和 Wiegold 在文献 [119] 研究了所有子群的自同构导子是大的群. Bechtell 等在文献 [21] 分类了所有交换子群的自同构导子是大的有限群. Deaconescu 等在文献 [56] 分类了所有非交换子群的自同构导子是大的有限群. Brandl 和 Deaconescu 在文献 [41] 分类了所有非交换子群的自同构导子是小的幂零群和非可解群. 李世荣在文献 [128] 确定了所有非极大交换子群的自同构导子是小的有限群, 他称这样的群为 NC 群. 安立坚等在文献 [2] 确定了所有非正规交换子群的自同构导子是小的有限群, 他们称这样的群为拟 NC 群. 本节主要介绍 NC p 群和拟 NC p 群的某些结果.

定理 14.2.1 设 G 是有限 p 群. 则 G 是 NC 群当且仅当 G 是交换的或 p^3 阶的非交换 p 群.

证明 明显地, 交换群和 p^3 阶的非交换 p 群是 NC 群. 反之, 若结论不成立, 设 G 是极小阶反例. 设 G 的所有极大子群是交换的. 则 G 可由两个元素 x, y 生成. 故 $|G/\Phi(G)| = p^2$, $\Phi(G) = Z(G)$ 且 $|\langle [x,y]\rangle| = p$. 因为 G 的指数为 p^2 的包含 $\langle [x,y]\rangle$ 的子群不是极大交换子群, 故所有这样的子群含在 $Z(G)$ 中. 这就迫使 $|G : \langle [x,y]\rangle| = p^2$. 从而 $|G| = p^3$. 矛盾. 故 G 有一个极大子群 H 是非交换的. 从而 $|H| = p^3$, 且由 G 的选择可得 $|G| = p^4$. 明显地, H 含有一个极大正规子群 K 使得 K 是 G 的正规子群. 于是 K 是 p^2 阶的极大交换子群. 由此可得 $|\mathrm{Aut}(K)_p| = p$. 这又得 $|G| \leqslant p^3$. 再一次推出矛盾. □

定理 14.2.2 设 G 是有限 p 群. 则 G 是拟 NC 群当且仅当 $|G'| \leqslant p$.

证明 $\Longleftarrow$: 若否, 则存在非正规交换子群 A 满足 $N_G(A) > C_G(A)$. 取 $a \in A$, $b \in N_G(A) \setminus C_G(A)$. 则 $1 \neq [a, b]$. 因为 $|G'| = p$, 故 $G' = \langle [a, b]\rangle$. 注意到 $[a, b] \in A$. 这推出 $A \trianglelefteq G$. 矛盾.

$\Longrightarrow$: 若结论不成立, 设 G 是极小阶反例. 则 $|G'| > p$ 且有以下结论.

(1) 若 $x, y \in G$ 满足 $\langle x, y\rangle < G$ 且 $[x, y] = c \neq 1$, 则 $c^p = 1$ 且 $c \in Z(G)$. 进一步地, 令 $A = \langle c, x\rangle$. 则 A 是 G 的交换正规子群.

事实上, 注意到 G 的子群也是拟 NC 群. 由 G 的极小性可得 $|\langle x, y\rangle'| \leqslant p$. 从而 $c^p = 1$. 取 $M \geqslant \langle x, y\rangle$ 且 $M \lessdot G$. 则 $M' = \langle c\rangle$. 因为 $M \trianglelefteq G$, 故 $M' \trianglelefteq G$. 从而 $c \in Z(G)$. 由此可得 $A = \langle c, x\rangle$ 交换. 因为 y 正规化但不中心化 A, 由拟 NC 群的定义可得 $A \trianglelefteq G$.

(2) 若存在 $z \in G$ 满足 $\langle x, z\rangle < G$ 且 $[x, z] = d \neq 1$, 则 $\langle d\rangle = \langle c\rangle$.

因为 $x \in A \trianglelefteq G$, 故 $d = [x, z] \in A$. 不妨设 $d = c^j x^i$. 由 (1) 可得 $d \in Z(G)$. 因而 $x^i \in Z(G)$. 若 $x^i = 1$, 则结论得证. 不妨设 $x^i \neq 1$. 取适当的 k 和 l 使得 $u = y^k z^l \neq 1$ 且 $[x, u] = x^i$. 因而 $u \in N_G(\langle x \rangle) \setminus C_G(\langle x \rangle)$. 由此可得 $\langle x \rangle \trianglelefteq G$. 于是 $c = [x, y] \in \langle x \rangle$ 且 $d = [x, z] \in \langle x \rangle$. 从而 $\langle d \rangle = \langle c \rangle$.

(3) $d(G) = 2$.

设 $d = d(G) > 2$. 令 $G = \langle g_1, g_2, \cdots, g_d \rangle$. 我们断言: 存在 G 的一个生成元集 $\{g_1', g_2', \cdots, g_d'\}$ 使得 $[g_i', g_{i+1}'] \neq 1$. 事实上, 因为 G 非交换, 取两个生成元不交换, 不妨设为 g_1' 和 g_2'. 若 $d = 3$, 那么第三个生成元, 比如说是 g_3, 它与 g_2' 交换. 令 $g_3' = g_3 g_1'$. 则结论成立. 对 d 作归纳. 不妨设 G 有生成元 $\{g_1', g_2', \cdots, g_d'\}$ 使得对于 $1 \leqslant i \leqslant d-2$ 均有 $[g_i', g_{i+1}'] \neq 1$. 若 $[g_d', g_{d-1}'] \neq 1$, 则结论得证. 若 $[g_d', g_{d-1}'] = 1$, 用 $g_d' g_{d-2}'$ 替换 g_d', 则结论也得证. 令 $M = \langle g_1', g_2', \cdots, g_{d-1}' \rangle$. 因为 $M < G$, 故 $|M'| = p$. 不妨设 $M' = \langle c \rangle$. 因为 $G' = \langle M', [g_d', g_i'] \mid 1 \leqslant i \leqslant d-1 \rangle$, 由 (2) 可得 $[g_d', g_i'] \in \langle c \rangle$. 于是就有 $G' = \langle c \rangle$. 矛盾.

(4) 令 $G = \langle a, b \rangle$. 则 $c(G) = 2$ 且 $|G'| = p^2$.

令 $[a, b] = c$ 且 $[c, a] = d$. 设 $d \neq 1$. 因为 $\langle a, c \rangle < G$, 由 (1) 可得 $d^p = 1$ 且 $d \in Z(G)$. 令 $A = \langle a, d \rangle$. 因为 $c \in N_G(A) \setminus C_G(A)$, 故 $A \trianglelefteq G$. 由此可得 $c = [a, b] \in A$. 从而 $[c, a] = 1$, 矛盾. 于是 $[c, a] = 1$. 对称地, $[c, b] = 1$. 因而 $c(G) = 2$ 且 $G' = \langle [a, b] \rangle$. 考虑 $\langle a^p, b \rangle < G$. 同样的论证给出 $[a^p, b]^p = 1$. 从而 $[a, b]^{p^2} = 1$. 这给出 $|G'| = p^2$.

(5) 最后的矛盾.

令 $H = \langle c^p, b \rangle$. 因为 $a^p \in N_G(H) \setminus C_G(H)$, 故 $H \trianglelefteq G$. 又 $c = (b^{-1})^a b$, 故 $c \in H$. 令 $c = b^i c^{jp}$. 则 $c^{1-jp} = b^i$. 这推出 $\langle c \rangle \leqslant \langle b \rangle$. 因而 $\langle b \rangle \trianglelefteq G$. 类似地, $\langle a \rangle \trianglelefteq G$. 因为 G 亚循环以及 a 和 b 的任意性, 有 G 的所有子群均正规. 因而 G 交换或是 8 阶的四元数群. 这与 $|G'| = p^2$ 矛盾. □

14.3　有限 p 群的余次数

Sanders 和 Wilde 在文献 [195] 引进了有限 p 群的余次数 (coexponent) 的概念: 设 G 是 p^n 阶群. 若 $\exp(G) = p^e$, 则称 $n - e$ 为 G 的**余次数**, 记为 $f(G)$. 对于奇阶 p 群, Sanders 和 Wilde[196] 证明了, $c(G) \leqslant 2f(G)$, 且若 $p \neq 3$, 则 $c(G) \leqslant 2f(G) - 1$. Sanders 在文献 [197] 进一步证明: 设 G 是有限 p 群且 $p > f(G) + 1$, 则 $c(G) \leqslant f(G) + 1$. 白华等在文献 [18] 改进了这个结果并对任意素数 p, 用余次数给出幂导 p 群的幂零类的最佳上界. 本节介绍文献 [18] 的工作.

引理 14.3.1　*若 G 为正则 p 群, $c(G) = f(G) + 1$. 则 $G/\mho_1(G)$ 是极大类的.*

证明 设 $\overline{G}=G/\mho_{e_2}(G)$. 由 [197] 中的命题 1 的证明可得, $c(\overline{G}/\mho_1(\overline{G}))=\omega_1(\overline{G})-1$. 因而 $\overline{G}/\mho_1(\overline{G})$ 为极大类群. 由于 $\mho_{e_2}(G)\leqslant\mho_1(G)$, 故 $\mho_1(\overline{G})=\overline{\mho_1(G)}$. 于是 $G/\mho_1(G)\cong\overline{G}/\overline{\mho_1(G)}=\overline{G}/\mho_1(\overline{G})$ 是极大类的. □

引理 14.3.2 *若 G 是有限 p 群, $f(G)\leqslant 2p-4$, 则 $c(G)\leqslant f(G)+1$.*

证明 若 $f(G)+1\leqslant p$, 则 $|G/\mho_1(G)|\leqslant p^n/p^{e(G)-1}=p^{f(G)+1}\leqslant p^p$. 因而 $\omega(G)\leqslant p-1$, 由 [89] 中的III, 定理 10.13 可知, G 正则. 下面假设 G 非正则且 $p-1\leqslant f(G)\leqslant 2p-4$.

由 [89] 中的III, 定理 10.14 可知, 存在 $N\lhd G$ 使得 $|N|=p^{p-1}$ 且 $e(N)=1$. 由于 $e(G/N)\geqslant e(G)-1$, 故

$$f(G/N)\leqslant n-(p-1)-(e(G)-1)=f(G)-p+2\leqslant p-2.$$

因此 G/N 正则且 $c(G/N)\leqslant f(G/N)+1\leqslant p-1$. 于是 $G_p(G)\leqslant N$.

由 [89] 中的III, 习题 27, $\overline{G}=G/N\times G/\mho_1(G)$ 正则. 设 $H=N\bigcap\mho_1(G)$, 则 $G/H\lesssim\overline{G}$, 进而 G/H 正则. 于是 $c(G/H)\leqslant f(G/H)+1$. 设 $|H|=p^r$, 则 $f(G/H)\leqslant f(G)-r+1$. 若 $c(G/H)\leqslant f(G/H)$, 则

$$c(G)\leqslant c(G/H)+r\leqslant (f(G)-r+1)+r=f(G)+1.$$

引理成立. 若 $c(G/H)=f(G/H)+1$, 则由引理 14.3.1 可知, $(G/H)/(\mho_1(G/H))$ 为极大类 p 群. 由于

$$\mho_1(G/H)\cong\mho_1(G)H/H=\mho_1(G)/H,$$

故 $G/\mho_1(G)$ 为极大类的正则 p 群. 由 [89] 中的III, 定理 14.21 可得, $|G/\mho_1(G)|\leqslant p^p$, 于是 $G_p\leqslant\mho_1(G)$.

由于 $|\mho_1(\mho_1(G))|\geqslant|\mho_2(G)|\geqslant p^{e(G)-2}$, 故

$$\omega(\mho_1(G))\leqslant(n-p)-(e(G)-2)=f(G)-(p-2)\leqslant p-2.$$

于是 $\mho_1(G)$ 正则且 $\log_p|\Omega_1(\mho_1(G))|=\omega(\mho_1(G))\leqslant f(G)-(p-2)$.

由于 $G_p\leqslant\mho_1(G)\bigcap N\leqslant\Omega_1(\mho_1(G))$, 故

$$c(G)+1-p\leqslant\log_p|G_p|\leqslant f(G)-(p-2).$$

因此 $c(G)\leqslant f(G)+1$. □

定理 14.3.3 *设 G 是有限 p 群, $p>2$, 则 $c(G)\leqslant f(G)+\max\left\{1,\left[\dfrac{f(G)-1}{p-2}\right]\right\}$.*

证明 对 $f(G)$ 作归纳.

若 $\left[\dfrac{f(G)-1}{p-2}\right] \leqslant 1$, 即 $f(G) \leqslant 2p-4$, 由引理 14.3.2 可知, 结论成立. 下设 G 非正则且 $\left[\dfrac{f(G)-1}{p-2}\right] \geqslant 2$. 由 [89] 中的III, 定理 10.14 可知, 存在 G 的正规子群 N 使得 $|N| = p^{p-1}$ 且 $e(N) = 1$. 由归纳假设可知,

$$c(G/N) \leqslant f(G/N) + \max\left\{1, \left[\frac{f(G)-1}{p-2}\right]\right\} \quad 且 \quad f(G/N) \leqslant f(G) - (p-2).$$

因此,

$$\begin{aligned} c(G) &\leqslant c(G/N) + (p-1) \leqslant f(G) - (p-2) + \max\left\{1, \left[\frac{f(G)-1}{p-2}\right]\right\} + (p-1) \\ &\leqslant f(G) + \max\left\{2, \left[\frac{f(G)-1}{p-2}\right]\right\} = f(G) + \max\left\{1, \left[\frac{f(G)-1}{p-2}\right]\right\}. \end{aligned}$$
□

引理 14.3.4 ([60] 或 [247]) 设 G 为 p 群, $M, N \lhd G$, 则下列叙述成立.

(1) 若 N 幂导嵌入于 G, 则对任意 $x \in G$, $\langle N, x\rangle$ 也幂导嵌入于 G;

(2) 若 M 和 N 幂导嵌入于 G, 则 $\mho_1(N), [M,N], MN, M\bigcap N$ 也幂导嵌入于 G;

(3) 若 G 是幂导 p 群, $G = \langle a_1, a_2, \cdots, a_d\rangle$, $d = d(G)$ 是 G 的最小生成元个数, 则 $\mho_i(G) = \{x^{p^i} \mid x \in G\} = \langle a_1^{p^i}\rangle\langle a_2^{p^i} \cdots a_d^{p^i}\rangle$, $0 \leqslant i \leqslant e(G)$;

(4) 若 N 幂导嵌入于 G 且存在 $S \subseteq G$ 使得 $N = \langle S^G\rangle$, 则 $N = \langle S\rangle$;

(5) 若 G 是幂导 p 群, $e = e(G)$, 则映射 $f: G \to G$, $f(x) = x^{p^{(e-1)}}$ 是同态映射. 进一步, 对 $1 \leqslant i \leqslant e$, 有 $(xy)^{p^i} \equiv x^{p^i}y^{p^i} (\mathrm{mod}\ \mho_{i+1}(G))$.

定义 14.3.5　设 G 为幂导 p 群, $d = d(G)$ 是 G 的最小生成数. 若 $G = \langle a_1, a_2, \cdots, a_d\rangle$ 且 $G = \langle a_1\rangle\langle a_2\rangle \cdots \langle a_d\rangle$, 则称集合 $(a_1, a_2, \cdots, a_d)$ 为 G 的一组基.

命题 14.3.6　若 G 是幂导 p 群, 则 G 存在一组基.

证明　对 $e = e(G)$ 作归纳. 若 $e = 1$, 由引理 14.3.4(3) 可知, 结论成立. 下设 $e > 1$. 设 $N = \mho_{e-1}(G)$. 由归纳假设, G/N 存在一组基 $(x_1N, x_2N, \cdots, x_dN)$. 再设 $N = \langle x_1^{p^{e-1}}\rangle \cdots \langle x_s^{p^{e-1}}\rangle$. 若 $s < d$, 对任意满足 $s < k \leqslant d$ 的 k, 设 $o(x_kN) = p^l$, 即存在 $y = y_k \in \langle x_1 \cdots x_s\rangle$ 使得 $x_k^{p^l} = y^{p^{e-1}}$. 由引理 14.3.4(5) 可得

$$(x_k y^{-p^{e-l-1}})^{p^l} = x_k^{p^l} y^{-p^{e-1}} = 1 \quad 且 \quad o(x_k y^{-p^{e-l-1}}) \leqslant p^l.$$

若 $o(x_k y^{-p^{e-l-1}}) < p^l$, 则

$$1 = (x_k y^{-p^{e-l-1}})^{p^{l-1}} \equiv x_k^{p^{l-1}} y^{-p^{e-2}} \quad (\mathrm{mod}\ \mho_l(\langle x_k\rangle \mho_{e-l-1}(G))).$$

由于 $\mho_l(\langle x_k\rangle\mho_{e-l-1}(G))=\langle x_k^{p^l}\rangle\mho_{e-1}(G)=\mho_{e-1}(G)$, 故

$$(x_kN)^{p^{l-1}}\in\langle x_1N,x_2N,\cdots,x_sN\rangle.$$

这与 $(x_1N,x_2N,\cdots,x_sN)$ 为 G/N 的一组基矛盾. 因而 $o(x_ky^{-p^{e-l-1}})=p^l$.

当 $i\leqslant s$ 时, 设 $a_i=x_i$. 当 $s<i\leqslant d$ 时, 设 $a_i=x_iy_i^{-p^{e-l-1}}$. 则

(1) $|G|=|\langle a_1\rangle||\langle a_2\rangle|\cdots|\langle a_d\rangle|$.

(2) 对任意 x_i, $1\leqslant i\leqslant d$, 有 $x_i\in\langle a_1,a_2,\cdots,a_d\rangle$.

因此 $G=\langle a_1,a_2,\cdots,a_d\rangle$, 进而 $G=\langle a_1\rangle\langle a_2\rangle\cdots\langle a_d\rangle$. 故 $(a_1,a_2,\cdots,a_d)$ 为 G 的一组基. □

引理 14.3.7 设 G 是二元生成的幂导 p 群, 则 G 亚循环.

证明 设 $G=\langle a,b\rangle$. 则 $G'=\langle [a,b]^G\rangle$. 由引理 14.3.4(4) 及 G' 幂导嵌入于 G 可得, $G'=\langle [a,b]\rangle$. 由于 $[a,b]\in\mho_1(G)=\{x^p\mid x\in G\}$, 故存在 $x\in G\setminus\mho_1(G)$ 使得 $[a,b]\in\langle x\rangle$. 因此 x 为 G 的生成元且 $\langle x\rangle\lhd G$. 于是 G 亚循环. □

定理 14.3.8 设 G 是幂导 p 群, 则当 $p>2$ 时, $c(G)\leqslant f(G)+1$, 当 $p=2$ 时, $c(G)\leqslant\left[\dfrac{f(G)}{2}\right]+1$.

证明 分两种情形证明.

(1) $p>2$.

若 $d(G)=2$, 则 G 亚循环, 因而 G 正则. 于是 $c(G)\leqslant f(G)+1$. 若 $d(G)>2$, 设 $(a_1,a_2,\cdots,a_d)$ 为 G 的一组基且 $o(a_1)\leqslant o(a_2)\leqslant o(a_d)$. 则 $o(a_1)=e_1=e(G)$, $o(a_2)=e_2$ 且 $\mho_{e_2}(G)=\langle a_1^{p^{e_2}}\rangle$ 为 G 的循环正规子群. 因而 $[G,G,\mho_{e_2}(G)]=1$. 由 [203] 可得

$$[\mho_{e_2}(G),G,G]=\mho_{e_2}([G,G,G])=[G,G,\mho_{e_2}(G)]=1.$$

由于 $G_{e_2+1}\leqslant\mho_{e_2}(G)$, 所以 $G_{(e_2+1)+2}(G)=1$. 于是 $c(G)\leqslant e_2+2$. 由于 $e_3\leqslant 1$, 故

$$f(G)=e_2+e_3+\cdots+e_d\geqslant e_2+1.$$

因此 $c(G)\leqslant f(G)+1$.

(2) $p=2$.

若 $d(G)\geqslant 3$, 类似于 $p>2$, $d\geqslant 3$ 的证明可得

$$[\mho_{e_2}(G),G,G]=\mho_{e_2}([G,G,G])=[G,G,\mho_{e_2}(G)]=1.$$

此时 $G_{[e_2/2]}\leqslant\mho_{e_2}(G)$. 因此 $c(G)\leqslant 1+[e_2/2]\leqslant 1+[f(G)/2]$.

若 $d(G)=2$, 则 G 亚循环. 故存在 $a,b\in G$ 使得

$$G=\langle a,b\mid a^{p^\alpha}=1,b^{p^\beta}=a^{p^\gamma},a^b=a^k\rangle,$$

其中

$$k^{p^\beta} \equiv 1 \pmod{p^\alpha}, \quad p^\gamma(k-1) \equiv 1 \pmod{p^\alpha}.$$

设 $t = (k-1)_p$. 则 $G' = \langle [a,b] \rangle = \langle a^{k-1} \rangle = \langle a^{p^t} \rangle$. 由于 G 幂导, 故 $t \leqslant 2$. 由于

$$G_{s+1} = [G_s, G] = \cdots = \langle a^{(k-1)^s} \rangle = \langle a^{p^{ts}} \rangle,$$

故 $c(G) \leqslant s$ 当且仅当 $\langle a^{p^{ts}} \rangle = 1$ 当且仅当 $ts \geqslant \alpha$. 由于 $|G| = p^{\alpha+\beta}$ 且 G 幂导, 故

$$e(G) = \max\{o(a), o(b)\} = \max\{\alpha, \alpha+\beta-\gamma\}.$$

因此 $f(G) = n - e = \min\{\beta, \gamma\}$.

由于 $k^{p^\beta} \equiv 1(\text{mod } p^\alpha)$, 故 $t+\beta \geqslant \alpha$. 由于 $p^\gamma(k-1) \equiv 1 \pmod{p^\alpha}$, 故 $t+\gamma \geqslant \alpha$. 不论哪种情形, 均有 $t + f(G) \geqslant \alpha$. 由于 $t \geqslant 2$, 故 $t(1+[f(G)/2]) \geqslant t + f(G) \geqslant \alpha$. 由上面内容可知, $c(G) \leqslant 1 + [f(G)/2]$. 定理得证. □

14.4 某些正则 p 群的分类及应用

众所周知, 正则 p 群在有限 p 群理论中占有十分重要的地位. 这是因为正则 p 群存在唯一性基底, 所以它们的分类问题要比一般的 p 群相对容易. 文献 [236],[242] 首次利用型不变量对某些正则 p 群进行了分类. 之后, 冀有虎等在文献 [107] 中分类了型不变量为 $(e,2,1)$ 的 p 群. 然而该文献的结果有某些疏漏, 张勤海等在文献 [270] 中继续文献 [236],[242],[107] 的工作. 更正了文献 [107] 的结果, 分别分类了型不变量为 $(e,1,1,1)$, $e \geqslant 2$ 和 $(1,1,1,1,1)$ 的正则 p 群. 作为这个分类的推论, 给出了 p^5 阶群的一个新的分类. 需要说明的是, p^5 阶群已被许多学者研究并分类, 例如, 文献 [17],[22],[59],[94],[95],[201]. 本节主要介绍文献 [270] 的工作.

14.4.1 型不变量为 $(e,1,1,1)$ 的正则 p 群的分类

本节我们将要给出型不变量为 $(e,1,1,1)$, $e \geqslant 2$ 的正则 p 群 G 的分类. 因为阶 $\leqslant p^p$ 的群是正则的, 所以为了确保得到的群一定正则, 我们假定 $e+3 \leqslant p$. 因为 $\omega(G) = 4$, 所以 $d(G) = 2,3,4$. 下面我们将用三个定理来考虑这三种情形. 由于篇幅所限, 下面只对 $d(G) = 2$ 的情形给予证明. 其余两种情形仅列出结果, 证明过程略去.

定理 14.4.1 设 $d(G) = 2$. 则 G 是亚交换群且同构于以下互不同构的群之一.

(Ⅰ) $\langle a,b,c,d \mid a^{p^e} = b^p = c^p = d^p = 1, [b,a] = c, [c,a] = 1, [c,b] = d, [d,a] = [d,b] = 1 \rangle$ ($|G'| = p^2$, $c(G) = 3$);

(Ⅱ) $\langle a,b,c,d \mid a^{p^e} = b^p = c^p = d^p = 1, [b,a] = c, [c,a] = d, [c,b] = 1, [d,a] = [d,b] = 1 \rangle$ ($|G'| = p^2$, $c(G) = 3$);

(Ⅲ) $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=d,[c,b]=a^{ip^{e-1}},[d,a]=[d,b]=1\rangle$ ($i=1$ 或 ν), 其中 ν 是一个固定的模 p 的平方非剩余, $|G'|=p^3$, $c(G)=3$;

(Ⅳ) $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=a^{p^{e-1}},[c,b]=d,[d,a]=[d,b]=1\rangle$ ($|G'|=p^3$, $c(G)=3$);

(Ⅴ) 当 $p\equiv 3 \pmod 4$ 时, $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=d,[c,b]=a^{ip^{e-1}},[d,a]=a^{p^{e-1}},[d,b]=1\rangle$, $i=0,1$ 或 ν, 其中 ν 是一个固定的模 p 的平方非剩余;

(Ⅵ) 当 $p\equiv 1 \pmod 4$ 时, $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=d,[c,b]=a^{ip^{e-1}},[d,a]=a^{p^{e-1}},[d,b]=1\rangle$, $i=0,1,\nu,\mu$ 或 ρ, 其中 $1,\nu,\mu$ 和 ρ 是由 $\mathbb{Z}_p^*$ 中四次剩余生成的子群 $\mathbb{F}$ 的陪集代表 ($|G'|=p^3$, $c(G)=4$);

(Ⅶ) 当 $p\equiv 2 \pmod 3$ 时, $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=a^{kp^{e-1}},[c,b]=d,[d,a]=1,[d,b]=a^{p^{e-1}}\rangle$ ($k=0$ 或 1);

(Ⅷ) 当 $p\equiv 1 \pmod 3$ 时, $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=a^{kp^{e-1}},[c,b]=d,[d,a]=1,[d,b]=a^{sp^{e-1}}\rangle$ ($k=0$ 或 1, $s=1,\mu$ 或 ν), 其中 $1,\mu$ 和 ν 是由 $\mathbb{Z}_p^*$ 中三次剩余生成的子群 $\mathbb{T}$ 的陪集代表 ($|G'|=p^3$, $c(G)=4$).

满足条件的互不同构的群共有 $6+\gcd(p-1,4)+2\gcd(p-1,3)$ 个, 即 (Ⅰ)—(Ⅷ).

证明 设 $\exp(G)=p^e$. 因为 $d(G)=2$, 所以 $|G/\Phi(G)|=p^2$. 取 G 的任一 L-群列:

$$G=L_0(G)>L_1(G)>L_2(G)>L_3(G)>L_4(G)=\mho_1(G).$$

因为 $\omega_1=4,\omega_2=\cdots=\omega_e=1$, 故

$$W_0(G)=L_4(G)=\mho_1(G),\quad W_1(G)=\cdots=W_{e-1}(G)=L_1(G),\quad W_e(G)=G.$$

因为 $L_1(G)$ 是 G 的极大子群, 所以不妨设 $L_2(G)=\Phi(G)$.

取 $a\in L_0(G)\backslash L_1(G)$, $b\in L_1(G)\backslash L_2(G)$ 且为最小阶元素, 则

$$o(a)=p^e,\quad o(b)=p,\quad G=\langle a,b\rangle.$$

令 $c=[b,a]$, 则 $c\neq 1$. 由 [247] 中的定理 5.4.17 及 $[b^p,a]=1$ 得 $c^p=[b,a]^p=1$, 即 $o(c)=p$. 由此可得 $\exp(G')=p$. 显然 $c\in L_2(G)=\Phi(G)$. 下面我们证明 $c\notin L_3(G)$. 若 $c\in L_3(G)$, 则 $c^g\in L_3(G)$, $\forall g\in G$. 从而可得 $G'\leqslant L_3(G)$, 则 $\Phi(G)\leqslant L_3(G)$, 矛盾. 所以 $c\in L_2(G)\backslash L_3(G)$.

因为 $\exp(G')=p$, 所以由 [247] 中的命题 5.1.13 得 G 是 p 交换的. 进一步有 $\mho_1(G)=\langle a^p\rangle\leqslant Z(G)$.

因为 G 的型不变量为 $(e,1,1,1)$, 所以 $|\mho_1(G)|=p^{e-1}$. 由 $d(G)=2$ 得 $G/\Phi(G)$ 的型不变量为 $(1,1)$. 由 [247] 中的引理 5.2.18 得, $\Phi(G)$ 的型不变量为 $(e-1,1,1)$

或 $(e,1)$. 若后者成立, 由 $\exp(G')=p$ 和 $\exp(\mho_1(G))=p^{e-1}$ 得

$$\exp(\Phi(G))=\exp(\mho_1(G)G')=p^{e-1}.$$

矛盾. 因此 $\Phi(G)$ 的型不变量为 $(e-1,1,1)$. 从而 $|G'|\leqslant p^3$. 我们断言 $|G'|>p$. 若否, 则 $G'=\langle c\rangle\leqslant Z(G)$. 从而 $\forall x\in G$ 可以表成下面的形式: $x=a^ib^jc^k$, 与 $\omega(G)=4$ 矛盾. 因此 $3\leqslant c(G)\leqslant 4$ 且 $|G'|=p^2$ 或 $|G'|=p^3$.

情形 1　$|G'|=p^2$.

因为 $\Phi(G)$ 的型不变量为 $(e-1,1,1)$ 且 $\exp(G')=p$, 故 $|G'\Omega_1(\mho_1(G))|=p^3$. 又因为 $|G'|=p^2$, 所以 $\Omega_1(\mho_1(G))=\langle a^{p^{e-1}}\rangle\nleqslant G'$. 由 $d(G)=2$ 得 G'/G_3 为循环群. 因而 $|G_3|=p$. 不妨设 $L_3(G)=\mho_1(G)G_3$. 令 $G_3=\langle d\rangle$, 则 (a,b,c,d) 是 G 的唯一性基底且 $G'=\langle c,d\rangle$. 由 $d\in Z(G)$, 显然可得

$$[d,a]=[d,b]=[d,c]=1.$$

进一步, 我们来考虑 $[c,a]$ 和 $[c,b]$.

若 $[c,b]\neq 1$, 则设 $[c,b]=d$. 令 $[c,a]=d^i$. 若 $p\mid i$, 则 G 为定理中的群 (Ⅰ). 若 $p\nmid i$, 令

$$a_1=ab^{-i},\quad c_1=[b,a_1],\quad [c_1,b]=d.$$

则 $[c_1,a_1]=1$. 从而 G 也为定理中的群 (Ⅰ).

若 $[c,b]=1$, 则 $[c,a]\neq 1$. 令 $d=[c,a]$. 则易得 G 为定理中的群 (Ⅱ).

下面我们来证明这两个群互不同构. 若其同构, 在群 (Ⅰ) 中, 设

$$a'=a^sb^tc^ud^m\, b'=a^{rp^{e-1}}b^vc^wd^n\quad 且\quad c'=[b',a'],$$

其中 s,t,u,m,r,v,w,n 为正整数且 $p\nmid s$, $p\nmid v$. 则 a', b', c' 满足群 (Ⅱ) 的定义关系. 特别地, $[c',b']=1$. 通过计算得

$$[c',b']=[b',a',b']=[a^{rp^{e-1}}b^vc^wd^n,\ a^sb^tc^ud^m,\ a^{rp^{e-1}}b^vc^wd^n]=[c,b]^{v^2s}=d^{v^2s}.$$

因此 $d^{v^2s}=1$. 则 $p\mid v$ 或 $p\mid s$, 矛盾.

情形 2　$|G'|=p^3$.

因为 $\Phi(G)$ 的型不变量为 $(e-1,1,1)$, 所以 $G'=\Omega_1(\Phi(G))\geqslant\langle a^{p^{e-1}}\rangle$. 我们断言 $\langle a^{p^{e-1}}\rangle\leqslant G_3$. 若否, 则

$$\mho_1(G)\bigcap G_c=\langle a^p\rangle\bigcap G_c=1,\quad 其中c=c(G),\quad 3\leqslant c\leqslant 4.$$

由于 $Z(G)\geqslant G_c\langle a^p\rangle$, 因此 $|Z(G)|\geqslant p^e$. 则 $|G/Z(G)|\lneqq p^3$ 且 $c(G)=3$. 又因为 G'/G_3 循环, 所以 $|G_3|=p^2$ 且 $G'/G_3=\langle\bar{c}\rangle$, 其中 $c=[b,a]$. 由 $a^{p^{e-1}}\in G'\backslash G_3$

和 $c\in G'\backslash G_3$ 可得, 对某个 i 有 $a^{ip^{e-1}}G_3=cG_3$. 则 $c^{-1}a^{ip^{e-1}}\in G_3\leqslant Z(G)$. 由 $\mho_1(G)\leqslant Z(G)$ 得, $c\in Z(G)$. 矛盾. 从而 $\langle a^{p^{e-1}}\rangle\leqslant G_3$.

因为 $|G_3|=p^2$, 所以 $|G_3\mho_1(G)|=p^e$. 不失一般性, 设 $L_3(G)=G_3\mho_1(G)$. 令 $G_3=\langle a^{p^{e-1}},d\rangle$, 其中 $o(d)=p$. 则 $d\in L_3(G)\backslash L_4(G)$ 且 (a,b,c,d) 是 G 的唯一性基底. 下面分两种情况考虑: (a) $c(G)=3$, (b) $c(G)=4$.

对于后者, 因为 $d\notin Z(G)$, 所以 $G_4=\langle a^{p^{e-1}}\rangle$. 显然因为无论哪种情况均有 $c(G)\leqslant 4$, 所以 G' 是交换群.

(a) $c(G)=3$.

由 $G_3\leqslant Z(G)$ 得 $[d,a]=[d,b]=1$. 因而 $[c,a]$, $[c,b]$ 生成 G_3. 由于 $|G_3|=p^2$, 因此 $[c,a]$ 和 $[c,b]$ 在 $G_3=\langle a^{p^{e-1}},d\rangle$ 中无关. 则对于某个整数 t, 用 ab^t 替换 a 且适当变换 d 后, 可设

$$[c,b]=a^{ip^{e-1}},\quad [c,a]=d,\quad 或\quad [c,b]=d,\quad [c,a]=a^{jp^{e-1}},$$

其中 $p\nmid i$, $p\nmid j$. 因此 G 同构于以下群之一:

(i) $\langle a,b,c,d\mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=d,[c,b]=a^{ip^{e-1}},[d,a]=[d,b]=[d,c]=1\rangle$, 其中 $p\nmid i$;

(ii) $\langle a,b,c,d\mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=a^{jp^{e-1}},[c,b]=d,[d,a]=[d,b]=[d,c]=1\rangle$, 其中 $p\nmid j$.

类似于情形 1, 可以证明对于任意的 i,j, 这两种群互不同构. 计算细节略.

下面确定群 (i) 和 (ii) 中互不同构的群的类型.

对于群 (i), 令 $b_1=b^\ell$, 则

$$[b_1,a]=c_1,\quad [c_1,a]=d_1,\quad [c_1,b_1]=a^{i\ell^2p^{e-1}},$$

其中 $c_1=c^\ell a^{ip^{e-1}\binom{\ell}{2}}$, $d_1=d^\ell$. 假定 ν 模 p 平方非剩余, 则 G 同构于以下群之一:

(ia) $\langle a,b,c,d\mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=d,[c,b]=a^{p^{e-1}},[d,a]=[d,b]=[d,c]=1\rangle$;

(ib) $\langle a,b,c,d\mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=d,[c,b]=a^{\nu p^{e-1}},[d,a]=[d,b]=[d,c]=1\rangle$.

类似于情形 1 的方法可证, 群 (ia) 和 (ib) 互不同构. 详细计算略. 综合群 (ia) 和 (ib), 可得 G 为定理中的群 (III).

对于群 (ii), 令 $b_1=b^\ell$, 则

$$[b_1,a]=c_1,\quad [c_1,a]=a^{p^{e-1}},\quad [c_1,b_1]=d_1,$$

其中 $j\ell\equiv 1(\mathrm{mod}\ p)$, $c_1=c^\ell d^{\binom{\ell}{2}}$, $d_1=d^{\ell^2}$. 则 G 为群 (IV).

综上可知, 在 (a) 中, G 同构于群 (III), (IV) 之一且其互不同构.

(b) $c(G)=4$, $G_4=\langle a^{p^{e-1}}\rangle$.

令 $\overline{G}=G/G_4$. 由 [247] 中的引理 5.2.18 得, $\overline{G}$ 的型不变量为 $(e-1,1,1,1)$ 或 $(e,1,1)$. 若后者成立, 则 $\exp(\overline{G})=p^e$. 另一方面, 由于 $\overline{G}=\langle\bar{a},\bar{b},\bar{c},\bar{d}\rangle$, $o(\bar{a})=p^{e-1}$ 且其余生成元的阶 $\leqslant p$, 因此 $\exp(\overline{G})=p^{e-1}$, 矛盾. 从而 $\overline{G}$ 的型不变量为 $(e-1,1,1,1)$. 进一步地, $c(\overline{G})=3$. 利用 (a) 的结果, $\overline{G}$ 同构于以下两种群之一:

(i°) $\langle\bar{a},\bar{b},\bar{c},\bar{d}\mid \bar{a}^{p^{e-1}}=\bar{b}^p=\bar{c}^p=\bar{d}^p=1,[\bar{b},\bar{a}]=\bar{c},[\bar{c},\bar{a}]=\bar{d},[\bar{c},\bar{b}]=1,[\bar{d},\bar{a}]=[\bar{d},\bar{b}]=[\bar{d},\bar{c}]=1\rangle$;

(ii°) $\langle\bar{a},\bar{b},\bar{c},\bar{d}\mid \bar{a}^{p^{e-1}}=\bar{b}^p=\bar{c}^p=\bar{d}^p=1,[\bar{b},\bar{a}]=\bar{c},[\bar{c},\bar{a}]=1,[\bar{c},\bar{b}]=\bar{d},[\bar{d},\bar{a}]=[\bar{d},\bar{b}]=[\bar{d},\bar{c}]=1\rangle$.

显然, 若 $e=2$, 则上面两种群同构于定理 2.4.2 中的群 $(15')$. 故 $e>2$. 因为 G' 是交换群, 所以 $[d,c]=1$. 进一步, 若 $[c,a]=d,[c,b]=a^{ip^{e-1}}$, 则

$$[d,b]=[c,a,b]=[c,b,a]=[a^{ip^{e-1}},a]=1.$$

类似地, 若 $[c,b]=d,[c,a]=a^{kp^{e-1}}$, 则

$$[d,a]=[c,b,a]=[c,a,b]=[a^{kp^{e-1}},b]=1.$$

因此, G 同构于下面的群之一:

(i) $\langle a,b,c,d\mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=d,[c,b]=a^{ip^{e-1}},[d,a]=a^{jp^{e-1}},[d,b]=[d,c]=1\rangle$, 其中 $p\nmid j$;

(ii) $\langle a,b,c,d\mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=a^{kp^{e-1}},[c,b]=d,[d,a]=1,[d,b]=a^{\ell p^{e-1}},[d,c]=1\rangle$, 其中 $p\nmid \ell$.

下面确定群 (i) 和 (ii) 中互不同构的群的类型.

因为 $c(G)=4$, 所以由命题 1.1.7(3) 和徐公式知, 对于任意的 $x_1,x_2,x_3,x_4\in G$ 和任意整数 n_1,n_2,n_3,n_4, 有

$$[x_1^{n_1},x_2^{n_2},x_3^{n_3},x_4^{n_4}]=[x_1,x_2,x_3,x_4]^{n_1n_2n_3n_4},\quad [x_1^{n_1},x_2^{n_2},x_3^{n_3}]\equiv[x_1,x_2,x_3]^{n_1n_2n_3}\ (\mathrm{mod}\ G_4). \tag{14.14}$$

在群 (i) 中, 令

$$a'=a^sb^tc^ud^m,\quad b'=a^{rp^{e-1}}b^vc^wd^n,$$

其中 s,t,u,m,r,v,w,n 是正整数且 $p\nmid s$, $p\nmid v$. 则 a', b' 生成 G. 令 $c'=[b',a']$. 因为 G 是亚交换群, 所以由徐公式和等式 (14.14) 知

$$\begin{aligned}c'&=[a^{rp^{e-1}}b^vc^wd^n,a^sb^tc^ud^m]\\&\equiv[b,a]^{vs}[b,a,a]^{v\binom{s}{2}+ws}=c^{vs}d^{v\binom{s}{2}+ws}\ (\mathrm{mod}\ G_4).\end{aligned}$$

则

$$[c',a']=[c^{vs}d^{v\binom{s}{2}+ws},a']$$
$$=d^{vs^2}a^{p^{e-1}(jvs\binom{s}{2}+j(v\binom{s}{2}+ws)s+ivst)}\notin Z(G).$$

因为在群 (ii) 中, $[c,a]\in Z(G)$, 所以 (i) 中任意群与 (ii) 中群均不同构. 令 $[c',a']=d'$. 通过计算有

$$[c',b']=a'^{iv^2p^{e-1}},\quad [d',a']=a'^{jvs^2p^{e-1}}.$$

因而, 对于任意的 j, s, 可适当选取 v 使得 $jvs^2\equiv 1(\mathrm{mod}\ p)$, 则 $[d',a']=a'^{p^{e-1}}$. 更有, 对于任意的平方剩余 (或平方非剩余) j, 当 s 取遍 $\mathbb{Z}_p^*$ 中所有的非零元时, v 取遍 $\mathbb{Z}_p^*$ 中所有平方剩余 (或平方非剩余). 从而 v^2 取遍 $\mathbb{Z}_p^*$ 四次剩余 (或平方非剩余的平方).

当 $p\equiv 3(\mathrm{mod}\ 4)$ 时, 因为平方剩余组成的集合与四次剩余组成的集合相同, 所以可以适当选择 v 使得 $[c',b']=a'^{ip^{e-1}}$, 其中 $i=0,1$ 或 ν, ν 是一个确定的平方非剩余. 从而得到三种互不同构的群:

$\langle a,b,c,d\mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=d,[c,b]=a^{ip^{e-1}},[d,a]=a^{p^{e-1}},[d,b]=[d,c]=1\rangle$ $(i=0,1,$ 或 $\nu)$, 其中 $p\equiv 3(\mathrm{mod}\ 4)$, ν 是一个确定的模 p 的平方非剩余. 得到群 (V).

当 $p\equiv 1(\mathrm{mod}\ 4)$, 由非零四次剩余组成的集合是乘群 $\mathbb{Z}_p^*$ 的指数为 4 的子群. 令 1, ν, μ, ρ 为该子群的陪集代表且 ν 为平方非剩余. 则有五种互不同构的群:

$\langle a,b,c,d\mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=c,[c,a]=d,[c,b]=a^{ip^{e-1}},[d,a]=a^{p^{e-1}},[d,b]=[d,c]=1\rangle,i=0,1,\nu,\mu$ 或 ρ, 其中 $p\equiv 1(\mathrm{mod}\ 4)$ 且 1, ν, μ 和 ρ 为由 $\mathbb{Z}_p^*$ 中非零四次剩余组成的子群 $\mathbb{F}$ 的陪集代表. 我们得到群 (VI).

对于群 (ii), 令 $a'=a^i$, $b'=b^j$, $p\nmid ij$, 则 $(a',b',c'=[b',a'],d'=[c',b'])$ 是 G 的另一组唯一性基底. 利用由命题 1.1.7(3) 和徐公式计算得

$$[d',b']=[b',a',b',b']=[b^j,a^i,b^j,b^j]=[b,a,b,b]^{ij^3}=a^{ij^3\ell p^{e-1}}=a'^{j^3\ell p^{e-1}},$$
$$[c',a']=[b',a',a']=[b^j,a^i,a^i]=[[b,a]^{ij}[b,a,a]^{j\binom{i}{2}}[b,a,b]^{i\binom{j}{2}},a^i]=[b,a,a]^{ji^2}$$
$$=a'^{kijp^{e-1}}.$$

设 $\mathbb{T}$ 是由 $\mathbb{Z}_p^*$ 中的三次剩余生成的子群. 则当 $p\equiv 2(\mathrm{mod}\ 3)$ 时, $\mathbb{T}=\mathbb{Z}_p^*$, 当 $p\equiv 1(\mathrm{mod}\ 3)$ 时, $|\mathbb{Z}_p^*:\mathbb{T}|=3$. 对于后者, 令 1, μ, ν 为 $\mathbb{Z}_p^*$ 的子群 $\mathbb{T}$ 的陪集代表. 所以对于群 (ii) 有下面两种情形: (a) $p\equiv 2(\mathrm{mod}\ 3)$, (b) $p\equiv 1(\mathrm{mod}\ 3)$.

情形 (a) 中, 对于任意的 ℓ, 可适当选择 j 使得 $\ell j^3\equiv 1(\mathrm{mod}\ p)$. 故 $[d',b']=a'^{p^{e-1}}$. 对于任意 k, 若 $p\nmid k$, 也可适当选择 i 使得 $kij\equiv 1(\mathrm{mod}\ p)$. 因此得到下面的群:

$\langle a', b', c', d' \mid a'^{p^e} = b'^p = c'^p = d'^p = 1, [b', a'] = c', [c', a'] = a'^{kp^{e-1}}, [c', b'] = d', [d', a'] = 1, [d', b'] = a'^{p^{e-1}}, [d', c'] = 1\rangle$ $(k = 0, 1)$ (两种群). 此为群 (Ⅶ).

情形 (b) 中, 对于任意的 ℓ, 可适当选择 j 使得 $\ell j^3 \equiv s \pmod p$, 其中 $s = 1$, μ 或 ν. 因此 $[d', b'] = a'^{sp^{e-1}}$. 同样, 当 $p \nmid k$ 时, 取适当的 i 使得 $kij \equiv 1 \pmod p$. 因而有下面的群:

$G(k, s) = \langle a', b', c', d' \mid a'^{p^e} = b'^p = c'^p = d'^p = 1, [b', a'] = c', [c', a'] = a'^{kp^{e-1}}, [c', b'] = d', [d', a'] = 1, [d', b'] = a'^{sp^{e-1}}, [d', c'] = 1\rangle (k = 0, 1, s = 1, \mu, \nu)$ (六种群). 此为群 (Ⅷ).

接下来证明不同的参数对应的群互不同构. 对于上面给出的群, 若 $k = 0$, 则 $C_G(\langle a'\rangle) = \langle a', c', d'\rangle$; 若 $k = 1$, 则 $C_G(\langle a'\rangle) = \langle a', d'\rangle$. 故 $k = 0$ 的群与 $k = 1$ 的群互不同构. 下面假定 $p \equiv 1 \pmod 3$. 将证明 s 取不同值时, 得到的群互不同构. 不妨设 $G(k, s_1) \cong G(k, s_2)$, 其中 $s_1, s_2 \in \{1, \mu, \nu\}$. 在群 $G(k, s_1)$ 中, 令

$$a'' = a'^m b'^n c'^u d'^v, \quad b'' = a'^{rp^{e-1}} b'^w c'^x d'^y,$$

其中 m, n, u, v, r, w, x, y 取适当的整数且 $p \nmid m$, $p \nmid w$ 使得 a'' 和 b'' 生成 $G(k, s_1)$, 并且

$$a'',\ b'',\ c'' = [b'', a''],\ d'' = [c'', b'']$$

满足群 $G(k, s_2)$ 的定义关系. 特别地, $[d'', b''] = a''^{s_2 p^{e-1}}$. 通过计算得

$$[d'', b''] = [b'', a'', b'', b''] = [b'^w, a'^m, b'^w, b'^w] = [b', a', b', b']^{mw^3} = a'^{s_1 mw^3 p^{e-1}},$$

$$a''^{p^{e-1}} = (a'^m b'^n c'^u d'^v)^{p^{e-1}} = a'^{mp^{e-1}}.$$

故 $[d'', b''] = a''^{s_1 w^3 p^{e-1}}$. 由上可得, $s_2 \equiv s_1 w^3 \pmod p$, 即 $s_1 = s_2$. □

定理 14.4.2 *设 $d(G) = 3$. 则 G 同构于以下互不同构的群之一.*

(Ⅸ) $\langle a, b, c, d \mid a^{p^e} = b^p = c^p = d^p = 1, [b, a] = d, [c, a] = [c, b] = 1, [d, a] = [d, b] = [d, c] = 1\rangle$ $(|G'| = p, c(G) = 2)$;

(Ⅹ) $\langle a, b, c, d \mid a^{p^e} = b^p = c^p = d^p = 1, [b, a] = [c, a] = 1, [c, b] = d, [d, a] = [d, b] = [d, c] = 1\rangle$ $(|G'| = p, c(G) = 2)$;

(Ⅺ) $\langle a, b, c, d \mid a^{p^e} = b^p = c^p = d^p = 1, [b, a] = a^{p^{e-1}}, [c, a] = d, [c, b] = 1, [d, a] = [d, b] = [d, c] = 1\rangle$ $(|G'| = p^2, c(G) = 2)$;

(Ⅻ) $\langle a, b, c, d \mid a^{p^e} = b^p = c^p = d^p = 1, [b, a] = 1, [c, a] = a^{p^{e-1}}, [c, b] = d, [d, a] = [d, b] = [d, c] = 1\rangle$ $(|G'| = p^2, c(G) = 2)$;

(ⅩⅢ) $\langle a, b, c, d \mid a^{p^e} = b^p = c^p = d^p = 1, [b, a] = 1, [c, a] = d, [c, b] = a^{p^{e-1}}, [d, a] = [d, b] = [d, c] = 1\rangle$ $(|G'| = p^2, c(G) = 2)$;

(XIV) $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=1,[c,a]=1,[c,b]=d,[d,a]=1,[d,b]=1,[d,c]=a^{p^{e-1}}\rangle$ $(|G'|=p^2, c(G)=3)$;

(XV) $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=1,[c,a]=a^{p^{e-1}},[c,b]=d,[d,a]=1,[d,b]=a^{p^{e-1}},[d,c]=1\rangle$ $(|G'|=p^2, c(G)=3)$;

(XVI) $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=d,[c,a]=[c,b]=1,[d,a]=1,[d,b]=a^{ip^{e-1}},[d,c]=1\rangle (i=1,\nu)$, 其中 ν 是一个固定的模 p 的平方非剩余 (两种群) $(|G'|=p^2, c(G)=3)$;

(XVII) $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=d,[c,a]=a^{p^{e-1}},[c,b]=1,[d,a]=1,[d,b]=a^{ip^{e-1}},[d,c]=1\rangle$ $(i=1,\nu)$, 其中 ν 是一个固定的模 p 的平方非剩余 (两种群) $(|G'|=p^2, c(G)=3)$;

(XVIII) $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=d,[c,a]=1,[c,b]=1,[d,a]=a^{p^{e-1}},[d,b]=[d,c]=1\rangle$ $(|G'|=p^2, c(G)=3)$;

(XIX) $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=d,[c,a]=1,[c,b]=a^{p^{e-1}},[d,a]=a^{p^{e-1}},[d,b]=[d,c]=1\rangle$ $(|G'|=p^2, c(G)=3)$.

满足条件的互不同构的群共有 11 个, 即 (IX)—(XIX).

定理 14.4.3 设 $d(G)=4$. 则 G 同构于以下互不同构的群之一.

(XX) $C_{p^e}\times C_p\times C_p\times C_p$ $(G'=1)$;

(XXI) $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=[c,a]=[c,b]=[d,a]=[d,c]=1,[d,b]=a^{p^{e-1}}\rangle$ $(|G'|=p, c(G)=2)$;

(XXII) $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=[c,a]=[c,b]=[d,b]=[d,c]=1,[d,a]=a^{p^{e-1}}\rangle$ $(|G'|=p, c(G)=2)$;

(XXIII) $\langle a,b,c,d \mid a^{p^e}=b^p=c^p=d^p=1,[b,a]=[c,a]=1,[d,a]=[c,b]=a^{p^{e-1}},[d,b]=[d,c]=1\rangle(|G'|=p, c(G)=2)$.

满足条件的互不同构的群共有 4 个, 即 (XIX)—(XXIII).

最后, 我们得到下面的定理.

定理 14.4.4 若 G 是正则 p 群, $p\geqslant 5$, 且其阶为 p^{e+3}, 型不变量为 $(e,1,1,1)$ $(e\geqslant 2)$, 则 G 同构于群 (I)—(XXIII) 之一且互不同构.

定理 14.4.1— 定理 14.4.3 中互不同构的群共有

$$23+\gcd(p-1,4)+2\gcd(p-1,3)\text{个}.$$

14.4.2 型不变量为 $(1,1,1,1,1)$ 的正则 p 群的分类

本节我们给出型不变量为 $(1,1,1,1,1)$ 的正则 p 群 $(p\geqslant 5)$ 的分类. 文献 [235] 已经得到了本节的结果. 这里我们用本书的方法给出了一个新的证明. 值得注意的是, 这里 G 的任意主群列都是 G 的一个 L-群列. 我们首先证明下面的引理.

引理 14.4.5　设 G 是型不变量为 $(1,1,1,1,1)$ 的非交换的正则 p 群. 若 $Z(G)\setminus G' \neq \varnothing$, 则 $G = Z \times H$, 其中 $1 \neq Z \leqslant Z(G)$ 且 $H \leqslant G$.

证明　因为 $\exp(G) = p$, 所以 $G' = \Phi(G)$. 任取非单位元 $z \in Z(G) \setminus G'$. 因为 $z \notin \Phi(G)$, 显然可取 $\{z, h_1, \cdots, h_s\}$ 为 G 的一个极小生成系. 令 $Z = \langle z \rangle$ 和 $H = \langle h_1, \cdots, h_s \rangle$, 则 $G = Z \times H$. □

定理 14.4.6　设 G 是型不变量为 $(1,1,1,1,1)$ 的正则 p 群. 则 G 同构于以下互不同构的群之一.

(Ⅰ) $d(G) = 5 : G$ 是 p^5 阶初等交换群.

(Ⅱ) $d(G) = 4$.

(Ⅱ-1) $G = \langle a,b,c,d,e \rangle = \langle c,d \rangle \times \langle a,b \rangle$, 其中, $\langle c,d \rangle \cong \mathrm{C}_p \times \mathrm{C}_p$ 且 $\langle a,b,e \mid a^p = b^p = e^p = 1, [b,a] = e \rangle$ 是方次数为 p 的 p^3 阶非交换群;

(Ⅱ-2) $G = \langle a,b,c,d,e \mid a^p = b^p = c^p = d^p = e^p = 1, [b,a] = [d,c] = e, [c,a] = [c,b] = [e,c] = [d,a] = [d,b] = [e,d] = [e,a] = [e,b] = 1 \rangle$ 是超特殊 p 群且写成 $\langle a,b \rangle$ 与 $\langle c,d \rangle$ 的中心积, 即 $\langle a,b \rangle * \langle c,d \rangle$.

(Ⅲ) $d(G) = 3$.

(Ⅲ-1) $G = \langle a,b,c,d,e \mid a^p = b^p = c^p = d^p = e^p = 1, [b,a] = d, [c,a] = e, [c,b] = [d,a] = [d,b] = [d,c] = [e,d] = [e,a] = [e,b] = [e,c] = 1 \rangle$ $(c(G) = 2)$;

(Ⅲ-2) $G = \langle a,b,c,d,e \rangle = \langle c \rangle \times \langle a,b,d,e \rangle$, 其中 $\langle c \rangle \cong \mathrm{C}_p$ 且 $\langle a,b,d,e \rangle$ 有如下定义关系: $a^p = b^p = d^p = e^p = 1, [b,a] = d, [d,a] = e, [d,b] = [e,a] = [e,b] = [e,d] = 1$ $(c(G) = 3)$;

(Ⅲ-3) $G = \langle a,b,c,d,e \mid a^p = b^p = c^p = d^p = e^p = 1, [b,a] = d, [d,a] = [c,b] = e, [d,b] = [c,a] = [d,c] = [e,a] = [e,b] = [e,c] = [e,d] = 1 \rangle$ $(c(G) = 3)$.

(Ⅳ) $d(G) = 2$.

(Ⅳ-1) $G = \langle a,b,c,d,e \mid a^p = b^p = c^p = d^p = e^p = 1, [b,a] = c, [c,a] = d, [c,b] = e, [d,a] = [d,b] = [d,c] = [e,d] = [e,a] = [e,b] = [e,c] = 1 \rangle$ $(c(G) = 3)$;

(Ⅳ-2) $G = \langle a,b,c,d,e \mid a^p = b^p = c^p = d^p = e^p = 1, [b,a] = c, [c,a] = d, [d,a] = e, [c,b] = [d,b] = [d,c] = [e,a] = [e,b] = [e,c] = [e,d] = 1 \rangle$ $(c(G) = 4)$;

(Ⅳ-3) $G = \langle a,b,c,d,e \mid a^p = b^p = c^p = d^p = e^p = 1, [b,a] = c, [c,a] = d, [c,b] = [d,a] = e, [c,d] = [d,b] = [e,a] = [e,b] = [e,c] = [e,d] = 1 \rangle$ $(c(G) = 4)$.

证明　因为 $|G| = p^5$, 所以 $|G'| \leqslant p^3$ 且 $c(G) \leqslant 4$. 根据 Burnside 的结果 (见 [89] 中的Ⅲ, 定理 7.8 b), G' 是交换群, 即 G 是亚交换群. 因为 $\omega(G) = 5$, 所以 $d(G) = 2, 3, 4, 5$.

若 $d(G) = 5$, 则 G 是初等交换 p 群, 从而 G 为定理中的群 (Ⅰ).

若 $d(G) = 4$, 则 $|G'| = p$. 分两种情况考虑: ① $Z(G) > G'$, ② $Z(G) = G'$.

若 $Z(G) > G'$, 由引理 14.4.5 知 $G = Z \times H$. 其中 $|Z| = p$, H 为 p^4 阶非交换群且 $|H'| = p$. 由定理 2.4.2 可知, H 是 C_p 与方次数为 p 的 p^3 阶非交换群的直积. 从而 G 为定理中的群 (Ⅱ-1).

若 $Z(G) = G'$, 显然 G 是超特殊 p 群, 因此 G 是两个方次数为 p 的 p^3 阶非交换群的中心积. 则 G 为定理中的群 (Ⅱ-2).

显然群 (Ⅱ-1) 与群 (Ⅱ-2) 互不同构.

若 $d(G) = 3$, 则 $|G'| = p^2$, $c(G) = 2$ 或 3.

当 $c(G) = 2$ 时, 令 $G = \langle a, b, c\rangle$, 则有 $G' = \langle [b,a], [c,a], [c,b]\rangle$. 不妨设 $d = [b,a]$, $e = [c,a]$ 且 d, e 生成 G'. 令 $[c,b] = d^ie^j$. 则 $[ca^i, ba^{-j}] = 1$. 分别用 ba^{-j}, ca^i 替换 b, c, 可知 G 为定理中的群 (III-1).

当 $c(G)=3$ 时, 显然 $|G_3| = p$. 下面分两种情况考虑: ① $Z(G) > G_3$, ② $Z(G) = G_3$.

情形 1 $Z(G) > G_3$.

因为 $c(G) = 3$, 所以 $Z(G) \neq G'$. 从而 $Z(G) \setminus G' \neq \varnothing$. 由引理 14.4.5 知 $G = Z \times H$, 其中 $|Z| = p$, H 为 p^4 阶非交换群且 $c(H) = 3$, $|H'| = p^2$. 由定理 2.4.2 知, H 是 p^4 阶群的列表中的群 (15′). 因此 G 为定理中的群 (III-2).

情形 2 $Z(G) = G_3$.

令 $\overline{G} = G/G_3$, 则 $c(\overline{G}) = 2$. 由定理 2.4.2 知 $\overline{G}$ 是 C_p 与方次数为 p 的 p^3 阶非交换群 $\overline{H}$ 的直积. 设 H 是 $\overline{H}$ 的原像. 则 $c(H) = 3$, 且 H 为定理 2.4.2 中 p^4 阶群的列表中的群 (15′). 设

$$
\begin{aligned}
H =& \langle a, b, d, e \mid a^p = b^p = d^p = e^p = 1, [b,a] = d, [d,a] = e,\\
& [d,b] = [e,a] = [e,b] = [e,d] = 1\rangle \quad \text{且} \quad G = \langle c\rangle H.
\end{aligned}
$$

则 $G_3 = H_3 = \langle e\rangle$. 再设 $[c,a] = e^i$ 且 $[c,b] = e^j$. 因为 $[c,ab] = e^{i+j} = [c,ba]$, 所以 $[c, b^{-1}a^{-1}ba] = [c,d] = 1$. 由 $c \notin Z(G)$ 知, i, j 中至少有一个不被 p 整除, 不妨记为 j. 用 c 的适当方幂替换 c 可使 $[c,b] = e$. 令 $a' = b^{-i}a$, 则 $[c,a'] = 1$, $[b,a'] = [b,a] = d$ 且 $[d,a'] = [d,a] = e$. 因此 G 为定理中的群 (III-3).

因为若 G 为群 (III-3), 则 $Z(G) = G_3$, 所以群 (III-2), (III-3) 互不同构.

若 $d(G) = 2$, 则 $|G'| = p^3$. 若 $c(G) = 2$, 则 $|G'| = p$, 矛盾. 因而 $c(G) = 3$ 或 4.

当 $c(G) = 3$ 时, 显然 G 是亚交换群, 设 $G = \langle a, b\rangle$ 且 $c = [b,a]$, 则 $G' = \langle [b,a], [c,a], [c,b]\rangle$. 因为 $|G'| = p^3$, 所以 $[b,a], [c,a], [c,b]$ 无关. 因此 G 为群 (VI-1).

当 $c(G) = 4$ 时, 显然 G 是极大类 p 群. 令 $\overline{G} = G/G_4$. 则 $\overline{G}$ 为定理 2.4.2 中 p^4 阶群的列表中的群 (15′). 设

$$
\overline{G} = \langle \bar{a}, \bar{b} \mid \bar{a}^p = \bar{b}^p = \bar{c}^p = \bar{d}^p = \bar{1}, [\bar{b}, \bar{a}] = \bar{c}, [\bar{c}, \bar{a}] = \bar{d}, [\bar{c}, \bar{b}] = \bar{1}\rangle, \quad G_4 = \langle e\rangle.
$$

则 (a,b,c,d,e) 是 G 的唯一性基底. 不妨设

$$[b,a]=c,[c,a]=d,\quad [c,b]=e^i,\quad [d,a]=e^j,\quad [d,b]=e^k.$$

因为 G 是亚交换群, 所以

$$[d,b]=[c,a,b]=[c,b,a]=[e^i,a]=1.$$

由此可得 $p\nmid j$. (若 $p\mid j$, 则 $[d,a]=[d,b]=1$, 由此得 $G_4=1$.) 因此, 用 e 的适当方幂替换 e 可使 $[d,a]=e$ 且 $[c,b]=e^{ij^{-1}}=e^{i'}$. 则有下面两种情形.

(1) $p\mid i'$;

(2) $p\nmid i'$.

若情形 (1) 成立, 显然 G 为群 (Ⅳ-1).

若情形 (2) 成立, 令 $b'=b^\ell$, $c'=[b',a]$, $d'=[c',a]$, 则由徐公式知

$$[c',b']=[b^\ell,a,b^\ell]=[c^\ell[c,b]^{\binom{\ell}{2}},b^\ell]=[c^\ell,b^\ell]=e^{i'\ell^2},$$

$$[d',a]=[b^\ell,a,a,a]=[d,a]^\ell=e^\ell.$$

令 $\ell=i'^{-1}$ 且 $e'=e^\ell$, 则 $[c',b']=e'$, 故 G 为群 (Ⅳ-3).

下证群 (Ⅳ-2), (Ⅳ-3) 互不同构. 若 G 为群 (Ⅳ-2), $\langle b,c,d,e\rangle$ 是 G 的交换的极大子群. 若 G 为群 (Ⅳ-3), 可证 G 没有交换的极大子群. (若否, 设 H 是 G 的交换的极大子群, 则 $\overline{H}$ 是 $\overline{G}$ 的交换的极大子群, 即 $\overline{H}=\langle\overline{b},\overline{c},\overline{d}\rangle$. 因为 H 只可能为 $\langle b,c,d,e\rangle$. 但 $\langle b,c,d,e\rangle$ 不是交换群, 矛盾.) □

14.4.3 p^5 阶群的分类 $(p\geqslant 5)$

根据 Hall 给出的正则 p 群的理论, 易知 $p^5(p>3)$ 阶群一定是正则群, 且存在唯一性基底和型不变量. 因此可以根据型不变量分类 p 群. 徐明曜在文献 [242] 中给出关于 P.Hall 基定理的一个构造性的证明和寻找唯一性基底的方法. 运用此种方法, 计算将被简化. James 在文献 [95] 中对正则的情况应用了型不变量的方法, 但是他主要运用的是 Hall 的同亲族思想.

设 G 是 p^5 阶群, 则 G 的型不变量可能为: (i) (5), (ii) (4,1), (iii) (3,2), (iv) (3,1,1), (v) (2,2,1), (vi) (2,1,1,1) 及 (vii) (1,1,1,1,1). 对于 (i), 易知 G 是循环群. 由 Huppert 的文献 [87] 知, 对于 (ii), (iii), G 是亚循环群. 徐明曜在文献 [242] 中解决了情形 (iv), 冀有虎等在文献 [107] 中解决了情形 (v). (事实上, 徐明曜和冀有虎等分别分类了型不变量为 $(e,1,1)$, $(e,2,1)$, $e\geqslant 2$ 的正则 p 群.) 最后两种情况已在前两节解决. 因此:

对于 (i), 有

(1) $G=\langle a \mid a^{p^5}=1\rangle \cong \mathrm{C}_{p^5}$.

对于 (ii) 和 (iii), 由文献 [87] 知, G 亚循环且由定理 6.1.3 知, G 同构于以下群之一.

(2) $\langle 2,0,0,1\rangle=\langle a,b \mid a^{p^3}=1, b^{p^2}=a^{p^2}, a^b=a^{1+p^2}\rangle$;

(3) $\langle 2,0,1,0\rangle=\langle a,b \mid a^{p^2}=1, b^{p^3}=1, a^b=a\rangle \cong \mathrm{C}_{p^2}\times \mathrm{C}_{p^3}$;

(4) $\langle 1,1,1,0\rangle=\langle a,b \mid a^{p^2}=1, b^{p^3}=1, a^b=a^{1+p}\rangle$;

(5) $\langle 1,1,0,1\rangle=\langle a,b \mid a^{p^3}=1, b^{p^2}=a^{p^2}, a^b=a^{1+p}\rangle$;

(6) $\langle 1,0,2,1\rangle=\langle a,b \mid a^{p^2}=1, b^{p^3}=a^p, a^b=a^{1+p}\rangle$;

(7) $\langle 1,0,3,0\rangle=\langle a,b \mid a^p=1, b^{p^4}=1, a^b=a\rangle \cong \mathrm{C}_p\times \mathrm{C}_{p^4}$.

对于 (iv), 由文献 [242] 知, G 同构于以下群之一.

(8) $\langle a,b,c \mid a^{p^3}=b^p=c^p=1, [b,a]=c, [c,a]=[c,b]=1\rangle$ $(d(G)=2)$;

(9) $\langle a,b,c \mid a^{p^3}=b^p=c^p=1, [b,a]=c, [c,a]=a^{p^2}, [c,b]=1\rangle$ $(d(G)=2)$;

(10) $\langle a,b,c \mid a^{p^3}=b^p=c^p=1, [b,a]=c, [c,a]=1, [c,b]=a^{p^2}\rangle$ $(d(G)=2)$;

(11) $\langle a,b,c \mid a^{p^3}=b^p=c^p=1, [b,a]=c, [c,a]=1, [c,b]=a^{\nu p^2}\rangle$, 其中 ν 是一个固定的模 p 的平方非剩余 $(d(G)=2)$;

(12) $\mathrm{C}_{p^3}\times \mathrm{C}_p\times \mathrm{C}_p$ $(d(G)=3)$;

(13) $\langle a,b,c \mid a^{p^3}=b^p=c^p=1, [b,a]=[c,a]=1, [b,c]=a^{p^2}\rangle$ $(d(G)=3)$;

(14) $\langle a,b,c \mid a^{p^3}=b^p=c^p=1, [b,a]=1, [c,a]=a^{p^2}, [b,c]=1\rangle$ $(d(G)=3)$.

对于 (v), 由文献 [107] 可知, G 同构于以下群之一①.

(15) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1, [b,a]=c, [c,a]=[c,b]=1\rangle$ $(d(G)=2)$;

(16) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1, [b,a]=c, [c,a]=1, [c,b]=b^p\rangle$ $(d(G)=2)$;

(17) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1, [b,a]=c, [c,a]=1, [c,b]=a^p\rangle$ $(d(G)=2)$;

(18) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1, [b,a]=c, [c,a]=1, [c,b]=a^{\nu p}\rangle$, 其中 ν 是一个固定的模 p 的平方非剩余 $(d(G)=2)$;

(19) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1, [b,a]=c, [c,a]=a^p, [c,b]=b^p\rangle$ $(d(G)=2)$;

(20) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1, [b,a]=c, [c,a]=b^{-p}, [c,b]=a^pb^{hp}\rangle$, $h=0,1,\cdots,\dfrac{p-1}{2}\left(d(G)=2, \dfrac{p+1}{2}\text{ 种群}\right)$;

(21) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1, [b,a]=c, [c,a]=b^{-\nu p}, [c,b]=a^{\nu p}b^{2\nu p}\rangle$, 其中 ν 是一个固定的模 p 的平方非剩余 $(d(G)=2)$;

(22) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1, [b,a]=c, [c,a]=b^{-p}, [c,b]=a^{\nu p}b^{hp}\rangle$, 其中 ν 是一个固定的模 p 的平方非剩余, $h=0,1,\cdots,\dfrac{p-1}{2}\left(d(G)=2, \dfrac{p+1}{2}\text{ 种群}\right)$;

(23) $\mathrm{C}_{p^2}\times \mathrm{C}_{p^2}\times \mathrm{C}_p$ $(d(G)=3)$;

(24) $\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1, [b,a]=[c,a]=1, [b,c]=a^p\rangle$ $(d(G)=3)$;

①文献 [14] 中遗漏了两种群.

(25) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [b, a] = [c, a] = 1, [b, c] = b^p \rangle$ $(d(G) = 3)$;

(26) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [b, a] = 1, [c, a] = a^p, [b, c] = b^{-p} \rangle$ $(d(G) = 3)$;

(27) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [b, a] = a^p, [c, a] = [b, c] = 1 \rangle$ $(d(G) = 3)$;

(28) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [b, a] = 1, [b, c] = a^p b^{hp}, [c, a] = b^p \rangle$, 其中 $h = 0, 1, \cdots, \dfrac{p-1}{2}$ $\left(d(G) = 3, \dfrac{p+1}{2} \text{ 种群} \right)$;

(29) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [b, a] = 1, [b, c] = a^p b^{hp}, [c, a] = b^{\nu p} \rangle$, 其中 $h = 0, 1, \cdots, \dfrac{p-1}{2}$, 其中 ν 是一个固定的模 p 的平方非剩余 $\left(d(G) = 3, \dfrac{p+1}{2} \text{ 种群} \right)$;

(30) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [b, a] = b^p, [b, c] = 1, [c, a] = a^p \rangle$ $(d(G) = 3)$;

(31) $\langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [b, a] = a^p, [b, c] = 1, [c, a] = b^p \rangle$ $(d(G) = 3)$.

(i)—(v) 中互不同构的群共有 $29 + 2p$ 个.

对于 (vi), G 同构于定理 14.4.1—定理 14.4.3 中所得群之一 (这里 $e = 2$). 互不同构的群共有 $23 + \gcd(p-1, 4) + 2\gcd(p-1, 3)$ 个.

对于 (vii), G 同构于定理 14.4.6 中所得群之一. 互不同构的群共有 9 个.

由此得到本节的基本定理.

定理 14.4.7 设 G 是 $p^5 (p \geqslant 5)$ 阶群, 则 G 同构于本节所给出的群之一. 共有 $61 + 2p + \gcd(p-1, 4) + 2\gcd(p-1, 3)$ 种互不同构的群.

14.5 平衡 p 群与 n 平衡 p 群

14.5.1 二元生成平衡 p 群

我们知道, 对有限群 G 的任意子群 H, K, 若 $K \leqslant N_G(H)$ 或 $H \leqslant N_G(K)$, 则 $HK = KH$. 反之则不成立. Blackburn, Deaconescu 和 Mann 在文献 [33] 中开始研究这样的群: 群 G 的任意子群 H, K, 只要 $HK = KH$ 就有 $K \leqslant N_G(H)$ 或 $H \leqslant N_G(K)$. 并称满足此条件的群为**平衡群**(equilibrated groups), 简称 **E 群**. 他们完全分类了有限非交换单 E 群, 刻画了可解但非幂零的有限 E 群, 并把有限幂零 E 群的研究化归为 p 群的情况. 对于奇素数 p 他们证明了如下定理.

定理 14.5.1 设 G 是 E-p 群, p 是奇素数. 若 $d(G) = 2$, 则下列之一成立:

(i) G 是类 2 亚循环群;

(ii) $|G| = p^3$ 并且 $\exp(G) = p$;

(iii) $|G| = p^4$, $c(G) = 3$ 且 G_1 不是初等交换的;

(iv) G 是极大类 3 群, $|G| = 3^n$ $(n \geqslant 5)$, 且当 n 为奇数时 G_1 交换.

在 (iii) 和 (iv) 中, G_1 是极大类 p 群 G 的基本子群, 它用下式定义: $G_1/G_4 = C_{G/G_4}(G_2/G_4)$.

在上述定理中, (ii)—(iv) 中的群确为平衡群. 但对 (i), 并非所有类 2 亚循环群都是平衡群. 另外, 对于 2 群的情形, 在文献 [33] 中只证明了每个极大类 2 群是平衡群, 没有更多的信息. Silberberg 在文献 [204] 中分类了有限二元生成平衡 2 群. 张勤海等在文献 [271] 中使用与 Silberberg 不同的方法给出了有限二元生成平衡 p 群的完全分类. 本节内容取自文献 [271].

首先, 我们证明二元生成平衡 2 群必亚循环, 于是无论对 p 是奇素数或 $p=2$, 都只需考虑亚循环的情况.

引理 14.5.2 ([204] 中的命题 3.1) *二元生成 E-2 群 G 必亚循环.*

证明 设 G 非亚循环. 则由定理 2.5.3 可知, $\overline{G}=G/\Phi(G')G_3$ 非亚循环. 因为 $|\overline{G}'|=2$, $\overline{G}$ 是内交换群. 由定理 1.7.10 可得, $\overline{G}\cong \mathrm{M}_2(n,m,1)$, 其中 $n\geqslant 2$, $m\geqslant 1$. 因为 $\mathrm{M}_2(n,m,1)/\langle a^4,b^2\rangle\cong \mathrm{M}_2(2,1,1)$, 又易验证 $\mathrm{M}_2(2,1,1)=\langle ab\rangle\langle a\rangle$, 且 $\langle ab\rangle$ 和 $\langle a\rangle$ 均非正规, $\mathrm{M}_2(2,1,1)$ 不是平衡群. 但易见平衡群的每个截断 (即子群的商群) 仍平衡, 矛盾. □

由引理 14.5.2, 对任意素数 p, 我们只需决定亚循环的 E-p 群.

我们先来决定内交换的亚循环 E-p 群. 首先证明几个引理.

引理 14.5.3 *设 G 是内交换 p 群. 若 p 为奇素数, 则 G 是 p 交换的; 若 $p=2$, 则 G 是 4 交换的.*

证明 由定理 1.7.7 可知 $|G'|=p$. 直接验证即得所需结果. □

引理 14.5.4 *设 G 是亚循环 p 群且 A 是 G 的满足 $A\not\leqslant\Phi(G)$ 的子群. 则下列结论等价: (1) $G'\leqslant A$. (2) $A\trianglelefteq G$. (3) $A\Phi(G')\trianglelefteq G$.*

证明 (1) $\Longrightarrow$ (2) 和 (2) $\Longrightarrow$ (3) 是显然的.

(2) $\Longrightarrow$ (1): 因为 $A\not\leqslant\Phi(G)$, 存在元素 $a\in A$, $b\in G$ 使得 $G=\langle a,b\rangle$. 因为 $A\trianglelefteq G$, 故 $G/A=\langle\bar{b}\rangle$. 于是得 $G'\leqslant A$.

(3) $\Longrightarrow$ (1): 因为 $A\Phi(G')\trianglelefteq G$, 由 (1) 与 (2) 的等价性得 $G'\leqslant A\Phi(G')$. 于是 $G'=G'\bigcap A\Phi(G')=\Phi(G')(G'\bigcap A)=G'\bigcap A$. 由此得 $G'\leqslant A$. □

引理 14.5.5 *设 G 是内交换的亚循环 p 群. 则 G 是平衡群当且仅当 G 同构于 Q_8 或 $\mathrm{M}_p(n,m)$. 对于后者, 或者 $n>m$, 或者 $n=m=p=2$.*

证明 $\Longleftarrow$: 容易验证 Q_8 是平衡群. 于是可设 $G\cong \mathrm{M}_p(n,m)$, 其中 $n>m$ 或者 $n=m=p=2$. 我们将证明 G 是平衡群. 因 G 极小非交换, 只需证明如果 $G=AB$, 则 A 或 B 是正规子群.

若 $n=m=p=2$, 则 $|G|=16$ 并且 G 中无 8 阶元. 假定 $G=AB$. 则 A 和 B 都是 4 阶的, 并且 $A\bigcap B=1$. 因为 a^2b^2 不是 G 中任意元素的平方, 每个 4 阶子群或包含 $G'=\langle a^2\rangle$, 或包含 $\langle b^2\rangle$. 因此 A 和 B 中必有一个包含 G', 则它在 G 中正规.

现在假定 $n > m$. 若 $n = 2$, 则 $m = 1$. 于是 G 是 p^3 阶的, 显然是平衡的. 若 $n \geqslant 3$, 令 $G = AB$. 则在 A 和 B 中至少有一个, 譬如 A 中存在元素 $b^j a^i$ 使 $(i,p) = 1$. 因 $|G'| = p$ 且 $n \geqslant 3$, 由引理 14.5.3 得, $(b^j a^i)^{p^{n-1}} = b^{jp^{n-1}} a^{ip^{n-1}} = a^{ip^{n-1}}$. 这推出 $G' \leqslant \langle b^j a^i \rangle$, 因此 A 在 G 中正规.

$\Longrightarrow$: 假定 G 不同构于 Q_8, 也不同构于 $M_p(n,m)$, 其中 $n = m = p = 2$ 或 $n > m$. 则 $G \cong M_p(n,m)$, 其中 $m \geqslant n$ 并且对 $p = n = 2$ 有 $m > 2$. 我们将找出两个非正规循环子群 $\langle x \rangle$ 和 $\langle y \rangle$ 使得 $G = \langle x \rangle \langle y \rangle$. 分下面两种情形.

情形 1　$m \geqslant n$ 且 $p \neq 2$, 或者 $m \geqslant n \geqslant 3$ 且 $p = 2$.

令 $x = b$, $y = ba$. 需证 $\langle x \rangle$ 和 $\langle y \rangle$ 都不在 G 中正规. 明显地, $\langle x \rangle \ntrianglelefteq G$. 为证 $\langle y \rangle \ntrianglelefteq G$, 由引理 14.5.3, 对任意正整数 k 有

$$y^{p^k} = (ba)^{p^k} = b^{p^k} a^{p^k}, \qquad \text{其中 } p \neq 2, \text{或者 } p = 2 \text{ 但 } k \geqslant 2. \tag{14.15}$$

若 $y^{p^k} \in \langle a \rangle$, 则 $k \geqslant m \geqslant n$ 且 $y^{p^k} = 1$. 因此 $\langle y \rangle \bigcap \langle a \rangle = 1$. 由引理 14.5.4, $\langle y \rangle$ 不在 G 中正规.

现证 $\langle x \rangle \langle y \rangle = G$. 由 (*) 式, 容易看出 $\langle y \rangle \bigcap \langle x \rangle = \langle y^{p^n} \rangle$. 因此, $|\langle y \rangle \langle x \rangle| = p^n |\langle x \rangle| = |G|$. 这推出 $\langle x \rangle \langle y \rangle = G$.

情形 2　$m > n = 2$ 且 $p = 2$.

令 $x = b$, $y = b^2 a$. 需证 $\langle x \rangle$ 和 $\langle y \rangle$ 都不在 G 中正规. 由引理 14.5.4 只需证 $\langle x \rangle \bigcap \langle a \rangle = 1$ 并且 $\langle y \rangle \bigcap \langle a \rangle = 1$. 第一式是显然的. 为证第二式, 首先容易验证 $b^2 \in Z(G)$. 而对任意的正整数 k, 又有 $y^{2^k} = (b^2 a)^{2^k} = b^{2^{k+1}} a^{2^k}$. 如果 $y^{2^k} \in \langle a \rangle$, 则 $k \geqslant m - 1 \geqslant 2$. 于是得 $\langle y \rangle \bigcap \langle a \rangle = 1$.

现在证 $\langle x \rangle \langle y \rangle = G$. 容易看出 $\langle y \rangle \bigcap \langle x \rangle = \langle y^{2^2} \rangle$. 于是 $|\langle y \rangle \langle x \rangle| = 2^2 |\langle x \rangle| = |G|$. 这推出 $\langle x \rangle \langle y \rangle = G$. □

我们通过下列两个步骤来决定亚循环 E-p 群: ① 决定具有下面的性质 P 的亚循环 p 群 G; ②证明在步骤①中得到的群 G 是平衡群.

性质 P　只要 G 表成子群 A 和 B 的乘积, 即 $G = AB$, 则 A 和 B 中至少有一个在 G 中正规.

引理 14.5.6　*设 G 是亚循环 p 群. 则 G 具有性质 P 当且仅当 $G/\Phi(G')$ 也具有性质 P.*

证明　$\Longleftarrow$: 若 G 不具有性质 P, 则存在 G 的两个非正规子群 A 和 B 满足 $G = AB$. 由引理 14.5.4, 可设 $A \geqslant \Phi(G')$, $B \geqslant \Phi(G')$. 于是 $G/\Phi(G') = A/\Phi(G') \cdot B/\Phi(G')$. 因为 A 和 B 在 G 中不正规, $A/\Phi(G')$ 和 $B/\Phi(G')$ 在 $G/\Phi(G')$ 中不正规. 因此 $G/\Phi(G')$ 不具有性质 P.

$\Longrightarrow$: 若 $G/\Phi(G')$ 不具有性质 P, 则存在 $G/\Phi(G')$ 的两个非正规子群 $A\Phi(G')$ 和 $B\Phi(G')$ 满足 $G/\Phi(G') = A/\Phi(G') \cdot B/\Phi(G')$. 因此 $G = AB$. 因为 $A/\Phi(G')$ 和

$B/\Phi(G')$ 在 $G/\Phi(G')$ 中不正规, A 和 B 也在 G 中不正规. 于是 G 不具有性质 P.□

定理 14.5.7 设 G 是亚循环 p 群. 则 G 具有性质 P 当且仅当 G 同构于下列群之一.

(1) 定理 6.1.3 中参数 $s=0$ 的群和定理 6.1.4 中参数 $s=0$ 的 (Ⅰ) 型群;

(2) 定理 6.1.4 中除了 (Ⅰ), (Ⅱ) 型群之外的群;

(3) 定理 6.1.4 中参数 $r=2, t=s=0$ 的 (Ⅱ) 型群.

证明 (1) 对于定理 6.1.3 中的群和定理 6.1.4 中的 (Ⅰ) 型群, 若 $s+u=0$, 则 G 交换, 当然具有性质 P. 下面假定 $s+u\neq 0$. 这时有 $\Phi(G')=\langle a^{p^{r+1}}\rangle$. 令 $x=a\Phi(G')$, $y=b\Phi(G')$. 则

$$G/\Phi(G')=\langle x,\ y \mid x^{p^{r+1}}=1,\ y^{p^{r+s+t}}=x^{p^{r+s}},\ [x,y]=x^{p^r}\rangle.$$

由引理 14.5.6, G 具有性质 P 等价于 $G/\Phi(G')$ 具有性质 P. 于是只需证 $G/\Phi(G')$ 具有性质 P 的充要条件为 $s=0$.

$\Longleftarrow$: 由引理 14.5.3, $G/\Phi(G')$ 是 p 交换或 4 交换的. 假定 $s=0$. 令 $x'=y^{-p^t}x$, 则 $x'^{p^r}=y^{-p^{r+t}}x^{p^r}=1$. 于是

$$G/\Phi(G')=\langle x',\ y \mid y^{p^{r+t+1}}=1,\ x'^{p^r}=1,\ [y,x']=y^{-p^{r+t}}\rangle,$$

由引理 14.5.5, $G/\Phi(G')$ 具有性质 P.

$\Longrightarrow$: 假定 $s\neq 0$. 则

$$G/\Phi(G')=\langle x,y \mid x^{p^{r+1}}=1, y^{p^{r+s+t}}=1, [x,y]=x^{p^r}\rangle.$$

因 $s\neq 0$, $r+s+t\geqslant r+1$. 据引理 14.5.5, $G/\Phi(G')$ 不具有性质 P.

(2) 对于定理 6.1.4 中的除了 (Ⅰ), (Ⅱ) 型群之外的群, 若 G 是二面体群、半二面体群或广义四元数群, 则 $G/\Phi(G')$ 是 8 阶二面体群或四元数群; 若 G 是通常亚循环群, 则 $G/\Phi(G')=G$. 在任何情况下, 由引理 14.5.5, $G/\Phi(G')$ 具有性质 P.

(3) 对于定理 6.1.4 中的 (Ⅱ) 型群, $\Phi(G')=\langle a^4\rangle$. 令 $x=a\Phi(G')$, $y=b\Phi(G')$. 则

$$G/\Phi(G')=\langle x,y \mid x^4=1, y^{2^{r+s+t}}=1, x^y=x^{-1}\rangle.$$

于是只需证 $G/\Phi(G')$ 具有性质 P 的充要条件为 $r+s+t=2$.

$\Longleftarrow$: 若 $r+s+t=2$, 则由引理 14.5.5, $G/\Phi(G')$ 具有性质 P, 再由引理 14.5.6, G 也具有性质 P.

$\Longrightarrow$: 假定 $r+s+t>2$. 则由引理 14.5.5, $G/\Phi(G')$ 不具有性质 P, 由引理 14.5.6, G 也不具有性质 P. □

定理 14.5.8 定理 14.5.7 中给出的群都是平衡群.

证明　只需证明定理 14.5.7 中给出的群的每个极大子群也具有性质 P. 并可设该极大子群非交换.

对定理 14.5.7 中的 (2) 型群, 它们的非循环极大子群也有循环极大子群, 因而也是 (2) 型群, 故具有性质 P.

对于 (1) 型群, 即具有下述定义关系的群:

$$G = \langle a, b \mid a^{p^{r+u}} = 1,\ b^{p^{r+t}} = a^{p^r},\ a^b = a^{1+p^r} \rangle,$$

其中 r, t, u 是非负整数, 且 $r \geqslant 1$ (或当 $p = 2$ 时 $r \geqslant 2$), $0 < u \leqslant r$. ($u = 0$ 对应于交换群.) 由计算可以看出对于奇素数 p, G 是 p^u 交换的, 而对于 $p = 2$, G 是 p^{u+1} 交换的. 又, 容易证明对于定理 6.1.3 中的群和定理 6.1.4 中的 (Ⅰ) 型群, 参数 $s = 0$ 等价于它们的最高阶循环子群包含导群. (其证明留给读者作为习题.) 如果 G 的极大子群的最高阶元素也是 G 的最高阶元, 则该极大子群具有性质 P. 因此, 为了证明 G 的所有极大子群具有性质 P, 我们只需考虑下列两种情形.

情形 1　$t = 0$ 且极大子群 $M_1 = \langle a^p, ba^{p-1} \rangle$.

这时 M_1 的最高阶循环子群是 $\langle a^p \rangle$ 和 $\langle ba^{(1+i)p-1} \rangle$, 其中 $0 \leqslant i \leqslant p-2$. 它们的阶是 p^{r+u-1}. 由计算得知这些子群包含 M_1'.

情形 2　$t > 0$ 且极大子群 $M_2 = \langle a, b^p \rangle$.

当 $t = 1$ 时, M_2 的最高阶循环子群是 $\langle a \rangle$ 和 $\langle b^p a^i \rangle$, 其中 $0 \leqslant i \leqslant p-2$. 当 $t \geqslant 2$, M_2 的最高阶循环子群是 $\langle b^p a^i \rangle$, i 是任意的非负整数. 由计算得知这些子群包含 M_2'.

对于 (3) 型群, $G = \langle a, b \mid a^{2^{v+t'+u+2}} = 1, b^{2^2} = a^{2^{v+t'+2}},\ a^b = a^{-1+2^{v+2}} \rangle$, 其中 v, t', u 是非负整数, $t' \leqslant 2, u \leqslant 1$, 且若 $t' \geqslant 1$, 则 $u = 0$. 该群 G 有 3 个极大子群:

$$M_1 = \langle a^2, b \rangle,\quad M_2 = \langle a, b^2 \rangle,\quad M_3 = \langle a^2, ba \rangle.$$

对 M_1, 令 $a^2 = a_1$. 则

$$M_1 = \langle a^2, b \rangle = \langle a_1, b \mid a_1^{2^{v+t'+u+1}} = 1, b^{2^2} = a_1^{2^{v+t'+1}}, a_1^b = a_1^{-1+2^{v+2}} \rangle,$$

且 $\Phi(M_1') = \langle a_1^{2^2} \rangle$. 若 $v + t' + u = 0$, 则 M_1 交换. 于是我们可假定 $v + t' + u \geqslant 1$.

假定 $v + t' \geqslant 1$. 令 $x = a_1\Phi(M_1')$, $y = b\Phi(M_1')$. 则

$$M_1/\Phi(M_1') = \langle x, y \mid x^{2^2} = 1, y^{2^2} = 1, [x, y] = x^2 \rangle.$$

它具有性质 P, 因此 M_1 也具有性质 P.

如果 $v + t' = 0$, 则 $u = 1$. 我们有

$$M_1 = \langle a_1, b \mid a_1^{2^2} = 1, b^{2^2} = a_1^2, a_1^b = a_1^{-1} \rangle.$$

令 $b_1 = b^2 a_1^{-1}$. 计算表明

$$M_1 = \langle b, b_1 \mid b^{2^3} = 1, b_1^2 = 1, [b, b_1] = b^{2^2} \rangle.$$

由引理 14.5.5, M_1 具有性质 P.

对 M_2, 令 $b^2 = b_1$. 则

$$M_2 = \langle a, b^2 \rangle = \langle a, b_1 \mid a^{2^{v+t'+u+2}} = 1, b_1^2 = a^{2^{v+t'+2}}, a^{b_1} = a^{1-2^{v+3}+2^{2v+4}} \rangle,$$

且 $\Phi(M_2') = \langle a^{2^{v+4}} \rangle$. 若 $t' + u \leqslant 1$, 则 $M_2' = \langle a^{2^{v+3}} \rangle = 1$, 于是 M_2 交换, 结论成立. 因此我们可设 $t' + u \geqslant 2$. 因为 $u \leqslant 1$, $t' \leqslant 2$, 得到 $t' = 2$ 或 1.

若 $t' = 2$, 令 $x = a\Phi(M_2')$, $y = b_1\Phi(M_2')$. 则

$$M_2/\Phi(M_2') = \langle x, y \mid x^{2^{v+4}} = 1, y^2 = 1, [x, y] = x^{2^{v+3}} \rangle.$$

由引理 14.5.5, $M_2/\Phi(M_2')$ 具有性质 P, 因此 M_2 也具有性质 P.

若 $t' = 1$ 且 $u = 1$, 有

$$M_2 = \langle a, b_1 \mid a^{2^{v+4}} = 1, b_1^2 = a^{2^{v+3}}, a^{b_1} = a^{1-2^{v+3}} \rangle.$$

令 $b_2 = b_1 a^{-2^{v+2}}$. 计算表明

$$M_2 = \langle a, b_2 \mid a^{2^{v+4}} = 1, (b_2)^2 = 1, [a, b_2] = a^{2^{v+3}} \rangle.$$

由引理 14.5.5, M_2 具有性质 P.

最后, 对于 $M_3 = \langle a^2, ba \rangle$, 令 $a^2 = a_1$, $ba = b_1$. 因为 $t' \leqslant 2$, $t' = 0, 1$ 或 2. 由类似的但更复杂的计算得到

$$M_3 = \begin{cases} \langle a_1, b_1 \mid a_1^{2^{v+t'+u+1}} = 1,\ b_1^{2^2} = a_1^{2^{v+1}(3-2^{v+3}+2^{2v+4})},\ [a_1, b_1] = a_1^{-2+2^{v+2}} \rangle, & t' = 0, \\ \langle a_1, b_1 \mid a_1^{2^{v+t'+u+1}} = 1,\ b_1^{2^2} = 1,\ [a_1, b_1] = a_1^{-2+2^{v+2}} \rangle, & t' = 1, \\ \langle a_1, b_1 \mid a_1^{2^{v+t'+u+1}} = 1,\ b_1^{2^2} = a_1^{2^{v+2}(3-2^{v+2}+2^{2v+3})},\ [a_1, b_1] = a_1^{-2+2^{v+2}} \rangle, & t' = 2. \end{cases}$$

若 $v + t' + u = 0$, 则 $M_3' = \langle a_1^2 \rangle = 1$, 因此 M_3 交换, 结论成立. 现在假定 $v + t' + u \geqslant 1$. 有 $\Phi(M_3') = \langle a_1^{2^2} \rangle$. 令 $x = a_1\Phi(M_3')$, $y = b_1\Phi(M_3')$. 则

$$M_3/\Phi(M_3') = \begin{cases} \langle x, y \mid x^{2^2} = 1, y^{2^2} = 1, [x, y] = x^2 \rangle, & t' = 1, 2 \text{ 或 } t' = 0 \text{ 且 } v \geqslant 1, \\ \langle x, y \mid x^{2^2} = 1, y^{2^2} = x^2, [x, y] = x^2 \rangle, & t' = v = 0. \end{cases}$$

对于 $t' = 1, 2$, 或者 $t' = 0$ 但 $v \geqslant 1$ 的情形, 由引理 14.5.5, $M_3/\Phi(M_3')$ 具有性质 P. 由引理 14.5.6 推出 M_3 具有性质 P.

对于 $t' = v = 0$ 的情形, 令 $y_1 = y^2 x^{-1}$, 计算表明

$$M_3/\Phi(M_3') = \langle y, y_1 \mid y^{2^3} = 1, y_1^2 = 1, [x, y] = y^{2^2} \rangle.$$

由引理 14.5.5, 它具有性质 P. 因此 M_3 也具有性质 P. □

14.5.2 n 平衡 p 群

设 G 是群. 称 G 为模群, 如果 G 的子群格是模格. 容易看出, 有限群 G 是模平衡群当且仅当对群 G 中的任意子群 H, K, 有 $H \leqslant N_G(K)$ 或 $K \leqslant N_G(H)$ 成立. 王娇等在文献 [222] 希望研究这样的有限 p 群 G, 即 G 中任意非循环子群 H, K 均有 $K \leqslant N_G(H)$ 或 $H \leqslant N_G(K)$. 为此, 他们引进了如下概念.

定义 14.5.9 称有限群 G 为 n 平衡群, 若对 G 中任意满足 $d(H) \geqslant n, d(K) \geqslant n$ 的子群 H, K 均有 $H \leqslant N_G(K)$ 或 $K \leqslant N_G(H)$.

显然, 有限群 G 是 1 平衡群当且仅当 G 是模平衡群. 而对于任意非循环子群 H, K 均有 $K \leqslant N_G(H)$ 或 $H \leqslant N_G(K)$ 的有限群 G 来说, G 恰是 2 平衡群. 文献 [222] 完全分类了二元生成 2 平衡 p 群, 对于生成元个数不小于 3 的 2 平衡 p 群 G, 也得到若干有趣的结果. 本节介绍他们的工作.

1. $d(G) = 2$ 的 2 平衡 p 群

引理 14.5.10 设 G 是 2 平衡 p 群, $H \leqslant G$, 且 $N \trianglelefteq G$. 则 H 和 G/N 也是 2 平衡 p 群.

证明 设 A 和 B 是 H 的非循环子群. 因 G 是 2 平衡 p 群, 故 $A \leqslant N_G(B)$ 或 $B \leqslant N_G(A)$. 从而 $A \leqslant N_H(B)$ 或 $B \leqslant N_H(A)$. 于是 H 是 2 平衡 p 群.

设 $\overline{G} = G/N$, 且 $\overline{K} = K/N$ 和 $\overline{L} = L/N$ 是 $\overline{G}$ 的非循环子群. 则 K 和 L 是非循环群. 于是 $\overline{K} \leqslant \overline{N_G(L)} = N_{\overline{G}}(\overline{L})$ 或 $\overline{L} \leqslant \overline{N_G(K)} = N_{\overline{G}}(\overline{K})$. 因此 G/N 是 2 平衡 p 群. □

引理 14.5.11 设 G 是 p 群. 若 $|G'| = p^3$, 则 G' 交换.

证明 由 G 是 p 群, $Z(G') > 1$. 若 $|Z(G')| = p$, 则根据 [26] 中的命题 1.13 可知 G' 循环. 若 $|Z(G')| > p$, 则显然 G' 交换, 引理得证. □

检查 p^4 阶群的分类 (定理 2.4.1 和定理 2.4.2)、亚循环 p 群的分类 (定理 6.1.4) 以及内交换 p 群的分类 (定理 1.7.10), 可得下列三个引理的结论. 证明细节略去.

引理 14.5.12 设 G 是非交换 2 平衡 p 群, $d(G) = 2$ 且 $|G| \leqslant p^4$.

若 $|G| = p^3$, 则 $G \cong Q_8$, $M_p(2,1)$ 或 $M_p(1,1,1)$, 其中 $p > 2$.

若 $|G| = p^4$, 且 G 亚循环, 则 $G \cong Q_{16}$, SD_{16}, $M_p(3,1)$ 或 $M_p(2,2)$.

若 $|G| = p^4$, 且 G 非亚循环, 则 G 是下列群之一:

(1) $M_p(2,1,1)$;

(2) $\langle a, b, c \mid a^9 = c^3 = 1, a^3 = b^3, [a,b] = c, [c,a] = 1, [c,b] = a^{-3} \rangle$;

(3) $\langle a, b, c \mid a^{p^2} = b^p = c^p = 1, [a,b] = c, [c,a] = a^p, [c,b] = 1 \rangle$, 其中 $p \geqslant 5$;

(4) $\langle a, b, c \mid a^{p^2} = b^p = c^p = 1, [a,b] = c, [c,a] = 1, [c,b] = a^{ip} \rangle$, 其中当 $p \geqslant 5$ 时, 则 $i = 1$ 或 i 为模 p 的平方非剩余, 当 $p = 3$ 时, 则 $i = 1$.

反之, 引理中的群为互不同构的 2 平衡 p 群.

引理 14.5.13 设 G 是亚循环 2 平衡 p 群且 $|G|=p^n$. 则 G 是下列群之一:

(1) Q_8;

(2) Q_{16};

(3) $M_2(n-1,1)$, 其中 $n\geqslant 3$;

(4) $M_2(2,n-2)$, 其中 $n\geqslant 4$;

(5) 型不变量为 $(2^{n-1},2)$ 的交换群;

(6) $\langle a,b\mid a^8=1,a^4=b^{2^{n-3}},[a,b]=a^2\rangle$, 其中 $n\geqslant 4$;

(7) 定理 6.1.4 中 $s\leqslant 1$ 的 (1) 型群和 (Ⅰ) 型群.

引理 14.5.14 设 G 是内交换非亚循环 2 平衡 p 群, 且 $|G|=p^n$. 则 $G\cong M_p(n-2,1,1)$, 且当 $p=2$ 时, 则 $n\geqslant 4$.

引理 14.5.15 设 G 是 2 平衡 p 群, $|G|=p^n$ 且 $d(G)=2$. 若 G 非亚循环, 则 $|G'|\leqslant p^2$.

证明 若否, 则 $|G'|\geqslant p^3$ 且 $n\geqslant 5$. 设 $N\leqslant G'$, $|N|=p$ 且 $N\trianglelefteq G$. 由 [26] 中的定理 36.1 和引理 14.5.10 可知, G/N 是非亚循环的 2 平衡 p 群. 由归纳, $|G'/N|\leqslant p^2$. 从而 $|G'|=p^3$. 设 $L\leqslant G'$, $|L|=p^2$, 且 $L\trianglelefteq G$. 令 $\overline{G}=G/L$. 由 [26] 中的定理 36.1 和定理 1.7.7, $\overline{G}$ 是内交换的非亚循环群. 又由引理 14.5.14 得 $\overline{G}\cong M_p(n-4,1,1)$, 其中若 $p=2$, 则 $n\geqslant 6$. 不妨设

$$\overline{G}=\langle \bar{a},\bar{b},\bar{c}\mid \bar{a}^{p^{n-4}}=\bar{b}^p=\bar{c}^p=\bar{1},[\bar{b},\bar{a}]=\bar{c},[\bar{c},\bar{a}]=[\bar{c},\bar{b}]=\bar{1}\rangle.$$

由引理 14.5.11, $G'=\langle c,L\rangle$ 为交换群. 下面分两种情形讨论.

情形 1 $p>2$.

假设 $L=\langle x\rangle$ 为循环群. 若 $o(c)=p^3$, 则由 [26] 中的定理 7.1 知, G 正则. 因为 $[b^{p^2},a]=1$, 故 $[b,a]^{p^2}=1$. 这与 $o(c)=p^3$ 矛盾. 于是 $c^p\in\langle x^p\rangle\leqslant Z(G)$. 从而 $[c^p,a]=[c^p,b]=1$. 这推出 $[c,a],[c,b]\in\langle x^p\rangle$. 进而得到 $x\notin G'$. 矛盾. 故 L 非循环. 于是存在 $y,z\in L$ 使得 $A=\langle a,y\rangle$ 与 $B=\langle b,z\rangle$ 非循环. 又 $[A,B]\nleqslant A$ 且 $[A,B]\nleqslant B$, 这与引理条件矛盾.

情形 2 $p=2$.

任取 $g\in L$, 设 $A=\langle a,g\rangle$, $B=\langle b,a^2\rangle$. 易知, $A\nleqslant N_G(B)$ 且 $B\nleqslant N_G(A)$. 于是 A 循环. 从而 $L\leqslant\langle a\rangle$ 为循环群. 设 $L=\langle x\rangle$, 则 $\langle a^{2^{n-4}}\rangle=\langle x\rangle$. 若 $c^2\in\langle x^2\rangle\leqslant Z(G)$, 则 $[c,a]$, $[c,b]\in\langle x^2\rangle$, 得到 $x\notin G'$, 矛盾. 故 $\langle c^2\rangle=\langle x\rangle$. 设 $[b,a]=c_1$. 因为 $[b^2,a]=c_1^2[c_1,b]=1$, 故 $[c_1,b]=c_1^{-2}$. 从而有 $[b,c^2]=[b,a^{2^{n-4}}]=c^4$. 另一方面, 因为 $[c^2,a]=1$, 故 $[c,a]=1$ 或 x^2. 这推出 $[b,a^4]=c^4$. 由此可知 $n=6$. 设 $H=\langle ab,a^4\rangle$, $K=\langle b,a^4\rangle$. 则 H 和 K 非循环. 但是 $H\nleqslant N_G(K)$ 且 $K\nleqslant N_G(H)$, 矛盾. □

定理 14.5.16　设 G 是 p 群, $|G| = p^n$ 且 $d(G) = 2$. 则 G 是 2 平衡 p 群当且仅当 G 是下列互不同构的群之一:

(1) 引理 14.5.13 中的群;

(2) $\mathrm{M}_p(n-2,1,1)$, 其中当 $p=2$ 时, 则 $n \geqslant 4$;

(3) $\langle a,b,c \mid a^8 = c^2 = 1, b^2 = a^4, [b,a] = c, [c,a] = a^4, [c,b] = 1\rangle$;

(4) $\langle a,b,c \mid a^{2^{n-2}} = b^2 = 1, c^2 = a^{2^{n-3}}, [b,a] = c, [c,a] = 1, [c,b] = c^2\rangle$, 其中 $n \geqslant 6$;

(5) $\langle a,b,c \mid a^{p^{n-2}} = b^p = c^p = 1, [b,a] = c, [c,a] = a^{p^{n-3}}, [c,b] = 1\rangle$, 其中当 $p \geqslant 5$ 时, 则 $n \geqslant 4$, 当 $p=3$ 时, 则 $n \geqslant 5$, 当 $p=2$ 时, 则 $n \geqslant 6$;

(6) $\langle a,b,c \mid a^9 = c^3 = 1, a^3 = b^3, [a,b] = c, [c,a] = 1, [c,b] = a^{-3}\rangle$;

(7) $\langle a,b,c \mid a^{p^{n-2}} = b^p = c^p = 1, [b,a] = c, [c,a] = 1, [c,b] = a^{ip^{n-3}}\rangle$, 其中当 $p \geqslant 5$ 时, 则 $n \geqslant 4$, $i = 1$ 或 i 为模 p 平方非剩余, 当 $p=3$ 时, 则 $n \geqslant 5$, $i=1$.

证明　若 $n \leqslant 4$, 由引理 14.5.12 知定理成立. 又由引理 14.5.13, 不妨设 $n \geqslant 5$ 且 G 非亚循环. 若 $|G'| = p$, 由定理 1.7.7 和引理 14.5.14 可得 G 同构于 (2) 型群. 于是由引理 14.5.15 可设 $|G'| = p^2$. 设 $N \leqslant G' \bigcap Z(G)$, 且 $|N| = p$. 令 $\overline{G} = G/N$, $N = \langle x\rangle$. 由 [26] 中的定理 36.1 可知, $\overline{G}$ 非亚循环. 因此 $\overline{G} \cong \mathrm{M}_p(n-3,1,1)$. 不妨设

$$\overline{G} = \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^{n-3}} = \bar{b}^p = \bar{c}^p = \bar{1}, [\bar{b},\bar{a}] = \bar{c}, [\bar{c},\bar{a}] = [\bar{c},\bar{b}] = \bar{1}\rangle.$$

再设 $A = \langle a, x\rangle$, $B = \langle b, a^{p^{n-4}}\rangle$. 则 $[A,B] \nleqslant A$ 且 $[A,B] \nleqslant B$. 于是 A 循环. 不妨设 $a^{p^{n-3}} = x$, $[b,a] = c$.

情形 1　$p = 2$.

若 $n=5$, 则 $a^4 = x$. 设 $C = \langle ab, c^2\rangle$, $D = \langle b, a^2\rangle$. 若 $c^2 = x$, 则 C 与 D 非循环. 易知 $[C,D] \nleqslant C$ 且 $[C,D] \nleqslant D$, 矛盾. 故 $c^2 = 1$. 由 $[b^2,a] = c^2[c,b] = 1$ 可得 $[c,b] = 1$. 又 $x \in G'$, 故 $[c,a] = x$. 若 $b^2 = x$, 则 G 同构于 (3) 型群. 若 $b^2 = 1$, 则 $o(ba^2) = 2$. 设 $H = \langle c, b\rangle$, $K = \langle ba^2, c\rangle$. 则 $[b,a^2] = a^4 \notin H$ 且 $a^4 \notin K$, 矛盾.

若 $n \geqslant 6$ 且 $b^2 = x$, 令 $b_1 = a^{2^{n-4}}b$. 则 $b_1^2 = 1$. 于是可设 $b^2 = 1$. 若 $c^2 = 1$, 由 $[b^2,a] = c^2[c,b] = 1$ 可得 $[c,b] = 1$. 从而 $[c,a] = x$. 此时, G 同构于 (5) 型群. 若 $c^2 = x$, 则 $[c,b] = c^2$. 若 $[c,a] = 1$, 则 G 同构于 (4) 型群. 若 $[c,a] = c^2$, 则 G 也同构于 (4) 型群.

情形 2　$p > 2$.

若 $b^p = x^t$, 令 $b_1 = a^{-tp^{n-4}}b$. 则 $b_1^p = 1$. 不妨设 $b^p = 1$. 计算可知, $[b^p,a] = c^p[c,b]^{\frac{p(p-1)}{2}}$. 从而 $c^p = 1$. 设 $[c,a] = x^i$, $[c,b] = x^j$. 若 $p \mid i, p \mid j$, 则 $x \notin G'$, 矛盾. 若 $p \nmid i, p \mid j$, 令 $b_1 = b^k$, $c_1 = c^k$, 其中 $ik \equiv 1 \pmod p$. 则 G 同构于 (5) 型群. 若 $p \mid i, p \nmid j$, 令 $b_1 = b^r$, $c_1 = [b^r, a]$, 其中 $p \nmid r$, 则 $[c_1, b_1] = a^{jr^2p^{n-3}}$. 于是 G 同构于

(7) 型群. 若 $p\nmid i, p\nmid j$, 令 $a_1=b^s a$, 其中 $sj\equiv -i \pmod p$, 则 $[c,a_1]=1$. 化为 $p\mid i$ 的情形.

容易看出, 定理中的群互不同构. 由引理 14.5.13, 只需验证定理中的 (2)—(7) 型群为 2 平衡 p 群.

若 G 同构于 (2) 型群, 不妨设

$$G=\langle a,b,c \mid a^{p^{n-2}}=b^p=c^p=1,[a,b]=c,[c,a]=[c,b]=1\rangle.$$

设 A, B 是 G 的非循环子群. 若 $ab^ic^j\in A$, 则 $|A|\geqslant p^{n-1}$. 从而 $A\trianglelefteq G$. 故可设 $A,B\leqslant\langle a^p,b,c\rangle$. 又因 $\langle a^p,b,c\rangle$ 交换, 于是 G 是 2 平衡 p 群. 同理, 若 G 同构于定理中的 (3)—(7) 型群, 则 G 也是 2 平衡 p 群. □

推论 14.5.17 设 G 是 2 平衡 p 群且 $d(G)=2$, 则下面结论成立.

(1) 若 $p>2$, 则 $|\Omega_1(G)|\leqslant p^3$;

(2) 若 G 非亚循环, 则 $|\Omega_1(\Phi(G))|=p^2$;

(3) 若 $\Omega_1(G)=G$, 则 $|G|\leqslant p^3$;

(4) 若 $\Omega_2(G)=G$, 则 $|G|\leqslant p^4$.

2. $d(G)\geqslant 3$ 的 2 平衡 p 群

引理 14.5.18 设 G 是 2 平衡 p 群. 若 G 是模群, 则 G' 循环.

证明 若 $\Phi(G')\neq 1$, 由归纳, 则 $G'/\Phi(G')$ 循环. 从而 G' 循环. 故可设 $\Phi(G')=1$ 且 $|G'|\geqslant p^2$. 设 $N\leqslant G'\bigcap Z(G)$ 且 $|N|=p$. 由归纳, G'/N 循环. 从而 $G'\cong \mathrm{C}_p\times\mathrm{C}_p$. 由文献 [93] 可设 $G=L\langle x\rangle$ 且 $L=\langle a\rangle\times\langle b\rangle$ 的型不变量为 (p^n,p^n), 其中当 $p=2$ 时, $n\geqslant 3$. 于是 $[a,x]=a^{p^{n-1}}$, $[b,x]=b^{p^{n-1}}$. 设 $A=\langle a,x\rangle$, $B=\langle b,x\rangle$. 因为 G 是 2 平衡 p 群, 有 $L\bigcap\langle x\rangle\neq 1$. 不妨设 $L\bigcap\langle x\rangle=\langle x^{p^v}\rangle$ 且 $a^{p^u}=x^{p^v}$.

若 $u<v$, 令 $a_1=ax^{-p^{v-u}}$. 则 $L\bigcap\langle a_1\rangle=1$. 设 $H=\langle a_1,b\rangle$, $K=\langle a_1,x\rangle$. 则 $[H,K]\ntrianglelefteq H$ 且 $[H,K]\ntrianglelefteq K$, 矛盾. 故 $u\geqslant v$. 若 $p>2$ 或 $u\geqslant 2$, 令 $x_1=a^{-p^{u-v}}x$. 若 $p=2$ 且 $u=1$, 令 $x_1=a^{2^{n-2}-1}x$. 容易看出 $L\bigcap\langle x_1\rangle=1$. 矛盾. □

引理 14.5.19 设 G 是 2 平衡 p 群. 若存在 $a,b\in G$ 使得 $\langle a,b\rangle$ 非亚循环, 则 $\Omega_1(G)=\Omega_1(\langle a,b\rangle)$.

证明 若否, 则存在 $c\in G\setminus\langle a,b\rangle$ 使得 $o(c)=p$. 设 $H=\langle a,b,c\rangle$, $A=\langle a,b\rangle$, $B=\langle b,c\rangle$. 因为 G 是 2 平衡 p 群, 故 $A\trianglelefteq H$ 或 $B\trianglelefteq H$. 若 $d(H)=2$, 由 [247] 中的习题 2.3.10 和引理 14.5.15 可知 $|A'|=p$. 从而 A 为内交换的非亚循环群. 进而 $r(A)=3$, $|\Omega_1(A)|=p^3$. 于是 $r(H)\geqslant 3$, $|\Omega_1(H)|\geqslant p^4$. 由定理 14.5.16 导出矛盾. 故 $d(H)=3$. 这推出 $H'\leqslant\Phi(A)$ 或 $H'\leqslant\Phi(B)$. 下面分两种情形讨论.

情形 1 $p>2$.

易知, A 同构于定理 14.5.16 中的 (2), (5), (6) 或 (7) 型群.

若 A 同构于定理 14.5.16 中的 (2), (5) 或 (7) 型群, 不妨设

$$A=\langle a,b,x \mid a^{p^n}=b^p=x^p=1,[b,a]=x,[x,a]=a^{ip^{n-1}},[x,b]=a^{jp^{n-1}}\rangle.$$

由推论 14.5.17 (3), $|\Phi(B)|\leqslant p$. 从而 $H'\leqslant\Phi(A)=\langle a^p,x\rangle$. 易知存在 $g\in\langle b,c\rangle\setminus\Phi(H)$ 使得 $[a,g]\in\langle a\rangle$. 任取 $h\in\langle a,g\rangle\setminus\Phi(H)$ 使得 $[b,h]\in\langle a\rangle$. 设 $C=\langle a,g\rangle$, $D=\langle b,h\rangle$. 则 $[a,b]\notin C$ 且 $[a,b]\notin D$, 矛盾.

若 A 同构于定理 14.5.16 中的 (6) 型群, 不妨设

$$A=\langle a,b,x \mid a^9=x^3=1,a^3=b^3,[a,b]=x,[x,a]=1,[x,b]=a^{-3}\rangle.$$

由推论 14.5.17 (4), $|\Phi(B)|\leqslant 9$. 从而 $H'=A'=\langle a^3,x\rangle$. 易知存在 $g\in\langle b,c\rangle\setminus\Phi(H)$ 使得 $[a,g]\in\langle a\rangle$. 若 $o(g)=9$, 计算可得 $\langle g^3\rangle=\langle a^3\rangle$. 从而可设 $g^3=a^3$. 令 $c_1=a^{-1}g$. 则 $o(c_1)=3$. 不妨设 $[a,c]\in\langle a\rangle$. 任取 $h\in\langle a,c\rangle\setminus\Phi(H)$ 使得 $[b,h]\in\langle a\rangle$. 设 $C=\langle a,c\rangle$, $D=\langle b,h\rangle$. 则 $D\nleqslant N_G(C)$ 且 $C\nleqslant N_G(D)$, 矛盾.

情形 2 $p=2$.

在此情形下, A 同构于定理 14.5.16 中的 (2)—(5) 型群之一. 若 A 同构于定理 14.5.16 中的 (2) 型群, 则设

$$A=\langle a,b,x \mid a^{2^n}=b^2=x^2=1,[b,a]=x,[x,a]=[x,b]=1\rangle,$$

其中 $n\geqslant 2$. 由推论 14.5.17 (3), $|\Phi(B)|\leqslant 2$. 从而 $H'\leqslant\Phi(A)=\langle a^2,x\rangle$. 进而 $[a^2,b]$, $[a^2,c]\in\langle a\rangle$. 设 $C=\langle a^2,b\rangle$, $D=\langle a^2,c\rangle$. 则 $[b,c]\in\langle a\rangle$. 易知存在 $g\in\langle b,c\rangle\setminus\Phi(H)$ 使得 $[a,g]\in\langle a\rangle$. 设 $E=\langle a,g\rangle$. 则 $E\nleqslant N_G(B)$ 且 $B\nleqslant N_G(E)$, 矛盾. 同理, 若 A 同构于定理 14.5.16 中的 (3)—(5) 型群之一, 则同样可得到矛盾. □

推论 14.5.20 *设 G 是 2 平衡 p 群且 $p>2$. 若 $d(G)=3$, 则 $|\Omega_1(G)|=p^3$.*

证明 若 G 不是模群, 由 [247] 中的习题 2.3.10、推论 14.5.17 (1) 和引理 14.5.19 可知 $|\Omega_1(G)|\leqslant p^3$. 再由文献 [118] 得到 $|\Omega_1(G)|=p^3$. 若 G 为模群, 由 [93] 有 $G'\leqslant\mho_1(G)$. 于是 $\Phi(G)=\mho_1(G)$. 又由 [26] 中的定理 7.1 和引理 14.5.18 得 G 正则. 于是 $|\Omega_1(G)|=|G/\mho_1(G)|=|G/\Phi(G)|=p^3$. □

由 [247] 中的推论 7.4.21, 文献 [118], 推论 14.5.17 (1) 和引理 14.5.19, 则有下面结论.

定理 14.5.21 *设 G 是 2 平衡 p 群, 且 $p>2$, 则下面结论成立.*

(1) 若 $|\Omega_1(G)|\geqslant p^4$, 则 G 为模群;

(2) 若 $d(G)\geqslant 4$, 则 G 为模群.

定理 14.5.22 *设 G 是 2 平衡 p 群且 $d(G)=3$. 则 G 中存在正规的亚循环子群 N 使得 G/N 循环.*

证明 设 $G=\langle a,b,c\rangle$, $H=\langle a,b\rangle$, $K=\langle a,c\rangle$. 因为 G 是 2 平衡 p 群, 于是 $H\trianglelefteq G$ 或 $K\trianglelefteq G$. 不妨设 $H\trianglelefteq G$ 且 H 非亚循环.

若 $|\Omega_1(H)|\geqslant p^3$, 由推论 14.5.17(2) 可知存在 $g,h\in H$ 使得 $o(g)=p$ 且 $H=\langle g,h\rangle$. 设 $A=\langle gh,c\rangle$, $B=\langle c,h\rangle$. 则 $g\notin A$ 且 $g\notin B$. 由引理 14.5.19 可知, A 和 B 亚循环. 又由 G 是 2 平衡 p 群, 不妨设 $A\trianglelefteq G$. 因此 G/A 循环.

若 $|\Omega_1(H)|<p^3$, 由引理 14.5.19 和推论 14.5.20 可得 $p=2$. 易知 H 同构于定理 14.5.16 中的 (3) 型群. 不妨设

$$H=\langle a,b,x\mid a^8=x^2=1,b^2=a^4,[b,a]=x,[x,a]=a^4,[x,b]=1\rangle.$$

则 $G'\leqslant\Phi(H)=\langle a^2,x\rangle$. 若 $[a,c]\notin\langle a\rangle$, 则 $[a,bc]\in\langle a\rangle$. 不妨设 $[a,c]\in\langle a\rangle$ 且 $[b,c]\in\langle a\rangle$. 从而 $K=\langle a,c\rangle$ 亚循环. 令 $C=\langle b,c\rangle$. 则可设 $C\trianglelefteq G$ 且 C 同构于定理 14.5.16 中的 (3) 型群. 进而得到 $o([b,c])=2$ 且 $[b,c]=a^4$. 又由 $[a^4,b]=[a^4,c]=1$ 可得 $C'\leqslant Z(C)$. 与 C 为定理 14.5.16 中的 (3) 型群矛盾. □

由 [27] 中的命题 73.9 易得下列的结论.

引理 14.5.23 设 G 是非 Dedekind 模 p 群, $|G'|=p$ 且 $d(G)\geqslant 3$. 若 G 是 2 平衡 p 群, 则 $G\cong \mathrm{M}_p(n,m)\times \mathrm{C}_{p^{e_1}}\times \mathrm{C}_{p^{e_2}}\times\cdots\times \mathrm{C}_{p^{e_t}}$, 其中 $t\geqslant 1, n>\{m,e_1,e_2,\cdots,e_t\}$, 且当 $p=2$ 时, $n\geqslant 3$.

定理 14.5.24 设 G 是 2 平衡 p 群, $d(G)\geqslant 4$ 且 $p>2$. 若 $\exp(G)=p^m$, 则对于 G 的任意一个阶为 p^m 的元 x, 均有 $G'\leqslant\langle x\rangle$.

证明 若 $|G'|=p$, 由定理 14.5.21 和引理 14.5.23 可知定理成立. 若 $m=1$, 由文献 [93] 和定理 14.5.21 可知 G 交换. 由引理 14.5.18 可设 $m\geqslant 2$, $G'=\langle y\rangle$ 且 $o(y)\geqslant p^2$. 令 $\overline{G}=G/\langle y^p\rangle$. 则 $|\overline{G}'|=p$. 若存在 $x\in G$ 且 $o(x)=p^m$ 使得 $G'\bigcap\langle x\rangle=1$, 则 $o(\bar{x})=\exp(\overline{G})=p^m$. 从而 $\overline{G}'\leqslant\langle\bar{x}\rangle$, 进而 $G'\leqslant\langle x\rangle$, 矛盾. 因此对于 G 的任意一个阶为 p^m 的元 x, 均有 $G'\bigcap\langle x\rangle\neq 1$. 设 $N\leqslant G'$ 且 $|N|=p$. 则 $\exp(G/N)=o(xN)=p^{m-1}$. 由归纳可得, $G'/N\leqslant\langle x\rangle/N$. 于是 $G'\leqslant\langle x\rangle$. □

3. $d(G)\geqslant 4$ 的 2 平衡 2 群

引理 14.5.25 设 G 是 2 平衡 2 群, $d(G)\geqslant 4$, $|G'|=4$, $N\leqslant G'\bigcap Z(G)$ 且 $|N|=2$. 若 G/N 是非 Dedekind 模 2 群, 则 G' 循环.

证明 设 $\overline{G}=G/N$, $N=\langle x\rangle$. 由引理 14.5.23 可设 $d(\overline{G})=4$,

$$\begin{aligned}\overline{G}=\langle \bar{a},\bar{b},\bar{c},\bar{d}\mid \bar{a}^{2^n}=\bar{b}^{2^m}=\bar{c}^{2^s}=\bar{d}^{2^t}=\bar{1},[\bar{a},\bar{b}]=\bar{a}^{2^{n-1}},\\ [\bar{c},\bar{a}]=[\bar{d},\bar{a}]=[\bar{c},\bar{b}]=[\bar{d},\bar{b}]=[\bar{c},\bar{d}]=\bar{1}\rangle,\end{aligned}$$

其中 $n\geqslant 3$. 假设 G' 非循环, 则 $o(a)=2^n$.

若 $c^{2^s}=d^{2^t}=1$, 则 $|\Omega_1(G)|>8$. 任取 $y,z\in G$, 由引理 14.5.19 推出 $\langle y,z\rangle$ 为交换群或为内交换的亚循环群. 于是 $[a,c]=[a,d]=1$. 设 $A=\langle b,c,d\rangle$, $B=\langle a,c\rangle$, $C=\langle a,d\rangle$. 因为 G 是 2 平衡 2 群, 故 $[b,c]=[b,d]=[c,d]=1$. 这推出 $|G'|=2$. 与引理条件矛盾. 若 $c^{2^s}=b^{2^m}=1$ 或 $d^{2^t}=b^{2^m}=1$, 同理可得矛盾.

若 $d^{2^t}=1$, 则 $b^{2^m}=c^{2^s}=x$. 当 $m>s$ 时, 令 $c_1=cb^{2^{m-s}}$. 当 $m<s$ 或 $s=m\geqslant 2$ 或 $s=m=1$, $[b,c]=1$ 时, 令 $b_1=bc^{2^{s-m}}$. 则 $c_1^{2^s}=1$ 或 $b_1^{2^m}=1$. 矛盾. 故可设 $m=s=1$ 且 $[b,c]=x$. 设 $D=\langle d,a^2b\rangle$, $E=\langle d,a^2c\rangle$. 由 G 是 2 平衡 2 群可知, 存在 $g\in\langle b,c\rangle$ 使得 $[d,g]=x$. 从而存在 $h\in\langle b,c\rangle$ 使得 $[d,ah]=1$. 设 $H=\langle ah,d\rangle$, $K=\langle b,c\rangle$. 则 $[H,K]\nleqslant H$, 且 $[H,K]\nleqslant K$, 矛盾. 因此 $d^{2^t}\neq 1$. 同理, $b^{2^m}\neq 1$, $c^{2^s}\neq 1$. 于是 $b^{2^m}=c^{2^s}=d^{2^t}=x$. 不妨设 $t=m=s=1$, $[b,c]=[b,d]=[c,d]=x$. 再令 $b_2=bcd$, 则 $b_2^2=1$. 矛盾. □

引理 14.5.26　*设 G 是非 Dedekind 2 群, $d(G)\geqslant 4$ 且 $|G'|=2$. 则 G 是 2 平衡 2 群当且仅当 G 为下列互不同构的群之一.*

(1) $\mathrm{M}_2(n,m)\times \mathrm{C}_{2^{e_1}}\times \mathrm{C}_{2^{e_2}}\times\cdots\times \mathrm{C}_{2^{e_t}}$, 其中 $t\geqslant 2$, $n>\max\{m,e_1,e_2,\cdots,e_t\}$, 且 $n\geqslant 3$;

(2) $\mathrm{D}_8*\mathrm{Q}_8$;

(3) $\mathrm{M}_2(2,1,1)*\mathrm{Q}_8$.

证明　若 G 为模群, 则由引理 14.5.23 可知 G 为 (1) 型群. 设 G 不是模群, 由 [247] 中的推论 7.4.21 可知, 存在 $a,b\in G$, 使得 $\langle a,b\rangle$ 不是通常亚循环群. 又由定理 14.5.16 可知, $\langle a,b\rangle\cong \mathrm{Q}_8$ 或 $\mathrm{M}_2(2,n)$ 或 $\mathrm{M}_2(m,1,1)$, 其中 $m\geqslant 2$. 任取 $x,y\in G$, 因 $|G'|=2$, 故 $[x,y^2]=1$. 这推出 $\Phi(G)\leqslant Z(G)$. 从而 $a\notin\Phi(G)$, $b\notin\Phi(G)$. 设 $d(G)=t+2$. 则存在 $x_1,x_2,\cdots,x_t$, 其中 $o(x_i)=2^{e_i}$, $1\leqslant i\leqslant t$, 使得 $G=\langle a,b,x_1,x_2,\cdots,x_t\rangle$. 不妨设 $e_1\geqslant e_2\geqslant\cdots\geqslant e_t$, $[x_i,a]=[x_i,b]=1$.

若 $\langle a,b\rangle\cong \mathrm{M}_2(m,1,1)$, 其中 $m\geqslant 2$, 不妨设

$$a^{2^m}=b^2=c^2=1,\quad [a,b]=c,\quad [c,a]=[c,b]=1.$$

由引理 14.5.19 得 $\Omega_1(G)=\langle a^{2^{m-1}},b,c\rangle$. 任取 $1\neq g\in G$, 则 $\langle g\rangle\bigcap\langle a,b\rangle\neq 1$. 设 $\langle x_i\rangle\bigcap\langle a,b\rangle=\langle x_i^{2^{v_i}}\rangle$, 其中 $1\leqslant i\leqslant t$. 若 $\langle x_i\rangle\bigcap\langle a,b\rangle\leqslant\langle a\rangle$, 则设 $x_i^{2^{v_i}}=a^{2^{u_i}}$. 当 $v_i\geqslant u_i$ 时, 令 $a_1=ax_i^{-2^{v_i-u_i}}$. 当 $v_i<u_i$ 时, 令 $x_i'=x_ia^{-2^{u_i-v_i}}$. 则 $\langle x_i'\rangle\bigcap\langle a,b\rangle=1$ 或 $\langle a_1\rangle\bigcap\langle a,b\rangle=1$, 矛盾. 故 $\langle x_i\rangle\bigcap\langle a,b\rangle\nleqslant\langle a\rangle$. 不妨设 $x_i^{2^{v_i}}=a^{2^{u_i}}c$. 令 $1\leqslant j\leqslant t$, $j\neq i$, $v_i\geqslant v_j$. 若 $v_i\geqslant 2$ 或 $[x_i,x_j]=1$, 令 $x_j'=x_jx_i^{2^{v_i-v_j}}$. 则 $\langle x_j'\rangle\bigcap\langle a,b\rangle\leqslant\langle a\rangle$, 矛盾. 于是 $x_i^2=a^{2^{u_i}}c$ 且 $[x_i,x_j]=c$. 这推出 $t=2$. 若 $u_i=1$, 则 $o(a^{-1}bx_i)=2$. 矛盾. 故 $u_i\geqslant 2$. 令 $x_i'=x_ia^{-2^{u_i-1}}$. 则 $x_i'^2=c$. 从而可设 $x_1^2=x_2^2=c$. 再设 $A=\langle a^2x_1,b\rangle$, $B=\langle a^2x_2,b\rangle$. 因 G 是 2 平衡 2 群, 故 $m=2$. 因此 $G\cong\mathrm{M}_2(2,1,1)*\mathrm{Q}_8$.

若 $\langle a,b\rangle \cong \mathrm{M}_2(2,n)$, 不妨设 $a^4 = b^{2^n} = 1, [a,b] = a^2$. 再设 $A = \langle ab, x_i\rangle$, $B = \langle b, x_i\rangle$, 其中 $1 \leqslant i \leqslant t$. 则 $1 \neq \langle x_i\rangle \bigcap \langle a,b\rangle \not\leqslant \langle b\rangle$. 于是可设 $\langle x_i\rangle \bigcap \langle a,b\rangle = \langle x_i^{2^{v_i}}\rangle$, 且 $x_i^{2^{v_i}} = a^2 b^{2^{u_i}}$. 从而得到 $v_i = 1$, $[x_i, x_j] = a^2$, 其中 $j \neq i$, $1 \leqslant j \leqslant t$. 进而推出 $t = 2$. 若 $n = 1$, 则 $G \cong \mathrm{D}_8 * \mathrm{Q}_8$. 设 $n \geqslant 2$. 若 $u_1 = u_2 = 1$, 则 $(x_1x_2)^2 = a^2b^4$. 不妨设 $u_1 \neq 1$. 当 $u_1 > 1$ 时, 令 $a_1 = ab^{2^{u_1-1}}x_1^{-1}$. 当 $u_1 = 0$ 时, 令 $a_1 = ab^{2^{n-1}}x_1^{-1}$. 则 $\langle a_1, b\rangle \cong \mathrm{M}_2(n,1,1)$. 于是 $G \cong \mathrm{M}_2(2,1,1) * \mathrm{Q}_8$.

若 $\langle a,b\rangle \cong \mathrm{Q}_8$, 任取 $g \in G \setminus \langle a, b, \Phi(G)\rangle$, 则 $\langle a,b\rangle \bigcap \langle g\rangle \leqslant \langle a^2\rangle$. 设 $o(g) = 2^k$. 若 $\langle a,b\rangle \bigcap \langle g\rangle = \langle a^2\rangle$, 则 $\langle ag^{2^{k-2}}, bg^{2^{k-2}}\rangle \cong \mathrm{M}_2(2,1)$. 故可设 $\langle a,b\rangle \bigcap \langle g\rangle = 1$. 于是对 $1 \leqslant i,j \leqslant t$ 且 $i \neq j$, $\langle x_i, x_j\rangle \not\cong \mathrm{Q}_8$. 不妨设 $\langle x_i, x_j\rangle$ 为通常亚循环群. 于是得到 $\langle x_i, x_j\rangle$ 交换. 从而可设 $\langle x_i\rangle \bigcap \langle x_j\rangle = 1$, $\langle a\rangle \bigcap \langle x_i, x_j\rangle = 1$. 再设 $A = \langle x_1 b, x_2\rangle$, $B = \langle x_1 a, x_2\rangle$. 由 G 是 2 平衡 2 群得 $o(x_1) = 2$. 故 $o(x_i) = 2$. 由此推出 G 是 Dedekind 群, 与引理条件矛盾.

容易看出, 引理中的群为互不同构的 2 平衡 2 群. □

引理 14.5.27 *设 G 是 2 平衡 2 群, $N \leqslant G' \bigcap Z(G)$ 且 $|N| = 2$. 则 G 中不存在商群 G/N 使得 $G/N \cong \mathrm{M}_2(2,1,1) * \mathrm{Q}_8$.*

证明 若否, 则设

$$\overline{G} = G/N = \langle \bar{a}, \bar{b}, \bar{c}, \bar{d} \mid \bar{a}^4 = \bar{b}^4 = \bar{c}^4 = \bar{d}^2 = \bar{1}, \bar{c}^2 = \bar{b}^2, [\bar{d}, \bar{a}] = \bar{b}^2, [\bar{c}, \bar{b}] = \bar{c}^2,$$
$$[\bar{a}, \bar{b}] = [\bar{a}, \bar{c}] = [\bar{b}, \bar{d}] = [\bar{c}, \bar{d}] = \bar{1}\rangle.$$

由 $[c^2, b] = c^4$ 得 $o(c) = o(b) = 4$. 从而 $\langle a, d\rangle$ 为内交换的非亚循环群. 由引理 14.5.14 和引理 14.5.19 可知 $\langle a, d\rangle \cong \mathrm{M}_2(n,1,1)$, 其中 $n \geqslant 2$ 且 $|\Omega_1(G)| = 8$. 若 $a^4 = 1$, 则 $d^2 = 1$, 推出 $|\Omega_1(G)| \geqslant 16$, 矛盾. 故 $a^4 \neq 1$. 若 $d^2 \neq 1$, 令 $d_1 = a^2 d$. 则 $d_1^2 = 1$. 不妨设 $d^2 = 1$, $c^2 = b^2$. 若 $[b,c] = b^2$, 则 $\langle b, c\rangle \cong \mathrm{Q}_8$. 设 $A = \langle b, c\rangle$, $B = \langle c^2, d\rangle$. 因为 G 是 2 平衡 2 群, 故 $[c,d] = [b,d] = 1$. 设 $H = \langle a^2 c, d\rangle$, $K = \langle a^2 b, d\rangle$. 则 $[H,K] \not\leqslant H$ 且 $[H,K] \not\leqslant K$, 矛盾. 若 $[b,c] = a^4 b^2$, 则 $\langle bc, a^2 b\rangle \cong \mathrm{Q}_8$, 同理得到矛盾. □

引理 14.5.28 *设 G 是 2 平衡 2 群, $|G| = 2^7$ 且 $d(G) \geqslant 4$, 则 $|G'| \leqslant 2$.*

证明 若否, 则 $4 \leqslant |G'| \leqslant 8$. 由引理 14.5.11 得 G' 交换.

情形 1 $|G'| = 4$.

设 $N \leqslant G' \bigcap Z(G)$ 且 $|N| = 2$. 令 $\overline{G} = G/N$. 由 [26] 中的命题 1.23 可设 $\overline{G}$ 非 Dedekind 群. 于是 $\overline{G}$ 同构于引理 14.5.26 中的 (3) 型群或 2^6 阶的 (1) 型群. 若 $\overline{G}$ 同构于 (1) 型群, 则 $\overline{G} \cong \mathrm{M}_2(3,1) \times \mathrm{C}_2 \times \mathrm{C}_2$. 由引理 14.5.25 得 G' 循环. 设

$$\mathrm{M}_2(3,1) = \langle \bar{a}, \bar{b} \mid \bar{a}^8 = \bar{b}^2 = \bar{1}, [\bar{a}, \bar{b}] = \bar{a}^4\rangle.$$

则 $G' = \langle a^4\rangle$, $o(a) = 16$. 从而 $[b^2, a] = a^8 \neq 1$, 矛盾. 若 $\overline{G}$ 同构于 (3) 型群, 由引理 14.5.27 同样可得矛盾.

情形 2 $|G'|=8$.

在这种情形下, $G'=\Phi(G)$ 且 $G'\cong \mathrm{C}_8$, $\mathrm{C}_4\times\mathrm{C}_2$ 或 $\mathrm{C}_2\times\mathrm{C}_2\times\mathrm{C}_2$.

若 $G'\cong\mathrm{C}_8$, 则存在 $a,b\in G$ 使得 $o([a,b])=8$. 从而 $|\langle a,b\rangle|=2^5$. 于是 $\langle a,b\rangle$ 为极大类群. 这与引理 14.5.13 的结论矛盾.

若 $G'\cong\mathrm{C}_4\times\mathrm{C}_2$, 则 $\exp(G)\leqslant 8$ 且存在 $a,b\in G$ 使得 $o([a,b])=4$. 因为 $|\langle a,b\rangle|\leqslant 2^5$, 由定理 14.5.16 可得, $\langle a,b\rangle\cong\mathrm{Q}_{16}$ 或同构于引理 14.5.13 中的 (6) 型群. 任取 $g\in G\setminus\langle a,b\rangle$, 设 $H=\langle a,b,g\rangle$. 若 $d(H)=2$, 则由 [247] 中的习题 2.3.10 可知 $|H'|\geqslant 8$. 又由 $|H|\leqslant 2^5$, 可得 H 为极大类群. 从而 $\exp(H)=16$, 矛盾. 于是 $d(H)=3$.

若 $\langle a,b\rangle\cong\mathrm{Q}_{16}$, 则设 $a^8=1,b^2=a^4,[a,b]=a^{-2}$. 易知存在 $c\in G\setminus\langle a,b\rangle$ 使得 $o(c)=2$. 设

$$L=\langle a,b,c\rangle,\quad A=\langle ab,c\rangle,\quad B=\langle b,c\rangle.$$

因为 $d(L)=3$, 得到 $L'\leqslant\Phi(A)$ 或 $L'\leqslant\Phi(B)$. 又由推论 14.5.17 (4) 得, $|\Phi(A)|\leqslant 4$, $|\Phi(B)|\leqslant 4$. 从而推出 $L'=\langle a^2\rangle$. 进而 A 或 B 同构于引理 14.5.13 中的 (6) 型群. 因此只需考虑 $\langle a,b\rangle$ 同构于引理 14.5.13 中的 (6) 型群. 设

$$a^8=1,\quad b^{2i}=a^4,\quad [a,b]=a^2,$$

其中 $i=1$ 或 2. 任取 $d\in G\setminus\langle a,b\rangle$, 设 $K=\langle a,b,d\rangle$. 若 $i=2$, 则 $K'\leqslant G'=\Phi(\langle a,b\rangle)$. 若 $i=1$, 则 $o(ba)=2$. 设 $C=\langle a,b\rangle$, $D=\langle ba,d\rangle$, 则 $K'\leqslant\Phi(C)$ 或 $K'\leqslant\Phi(D)$. 因为 $\Omega_1(\langle a,b\rangle)$ 非交换, 由引理 14.5.19 可知 D 不是内交换的非亚循环群. 验证定理 14.5.16 中的群易知 $|\Phi(D)|\leqslant|\Phi(C)|=4$. 从而 $K'=\langle a^2\rangle$. 于是, 对 $i=1$ 或 2, 都可得到 $K'\leqslant\langle a^2,b^2\rangle$. 由 $[a,b]=a^2$, 不妨设 $[a,d]$, $[b,d]\in\langle b^2\rangle$. 从而 $[d^2,b]=1$. 再设 $E=\langle b,d\rangle$. 则 $b\in C_K(\Phi(D))\bigcap C_K(\Phi(E))$. 因为 G 是 2 平衡 2 群, 推出 $a^2\in\Phi(D)$ 或 $a^2\in\Phi(E)$. 又由 $[a^2,b]\neq 1$, 矛盾.

若 $G'\cong\mathrm{C}_2\times\mathrm{C}_2\times\mathrm{C}_2$, 则 $\exp(G)=4$. 任取 $x,y\in G$, 由推论 14.5.17 (4) 有 $|\langle x,y\rangle|\leqslant 2^4$. 从而 $|\langle x,y\rangle'|\leqslant 2$. 于是 $G'=\Phi(G)\leqslant Z(G)$. 若 $\langle x,y\rangle$ 为内交换的非亚循环群, 由引理 14.5.14 和引理 14.5.19 可知, $G'=\Omega_1(G)=\Omega_1(\langle x,y\rangle)\nleqslant Z(G)$. 矛盾. 于是 $\langle x,y\rangle$ 为内交换的亚循环群或交换群. 设

$$G=\langle a,b,c,d\rangle,\quad A=\langle a,b,c\rangle,\quad B=\langle a,b,d\rangle.$$

因为 G 是 2 平衡 2 群, 可设 $A\trianglelefteq G$, $\langle a,b\rangle\trianglelefteq A$. 从而 $G'\leqslant\Phi(A)$. 进而 $|A|=2^6$. 于是 $|\langle a,b\rangle|=2^4$, $o(c)=4$ 且 $\langle a,b\rangle\bigcap\langle c\rangle=1$. 若 $[a,b]\neq 1$, 则 $\langle a,b\rangle\cong\mathrm{M}_2(2,2)$. 设 $[a,b]=a^2$, $C=\langle ab,c^2\rangle$, $D=\langle b,c^2\rangle$. 则 $[C,D]\nleqslant C$ 且 $[C,D]\nleqslant D$. 矛盾. 故 $[a,b]=1$. 同理, 由 $[a,c]=[b,c]=1$ 得 A 交换. 再设 $H=\langle b,c,d\rangle$, $K=\langle a,c,d\rangle$. 则不妨设 $H\trianglelefteq G$. 类似可证 H 交换. 这推出 $|G'|\leqslant 2$. 矛盾. □

定理 14.5.29 设 G 是 2 平衡 2 群, $|G|=2^n$, $d(G)\geqslant 4$ 且 $n\geqslant 7$, 则 G' 循环.

证明 若 $n=7$, 由引理 14.5.28 可知定理成立. 设 $n\geqslant 8$ 且 $|G'|\geqslant 4$. 若 $\Phi(G')\neq 1$, 则取 $H\leqslant \Phi(G')\bigcap Z(G)$, 且 $|H|=2$. 归纳可得 G'/H 循环, 从而 G' 循环. 若 $\Phi(G')=1$, 则 G' 初等交换. 任取 $N\leqslant G'\bigcap Z(G)$ 且 $|N|=2$. 归纳可得 G'/N 循环, 从而 $G'\cong \mathrm{C}_2\times \mathrm{C}_2$. 由 [26] 中的命题 1.23, 不妨设 G/N 为非 Dedekind 2 群. 于是 G/N 同构于引理 14.5.26 中的 (1) 型群. 再由引理 14.5.25 可得 G' 循环. 矛盾. □

定理 14.5.30 设 G 是非 Dedekind 2 平衡 2 群, $|G|=2^n$, $d(G)\geqslant 4$, 且 $n\geqslant 7$. 若 $|G'|=2^m$, 则 $G\cong\langle a,b,x_1,x_2,\cdots,x_t\mid a^{2^u}=b^{2^v}=x_1^{2^{e_1}}=x_2^{2^{e_2}}=\cdots=x_t^{2^{e_t}}=1,[b,a]=a^{2^{u-m}},[x_i,a]=[b,x_i]=[x_i,x_j]=1\rangle$, 其中 $1\leqslant i,j\leqslant t$, $i\neq j$, $t\geqslant 2, v\geqslant m$, $u-m\geqslant\{v,e_1,e_2,\cdots,e_t\}$, 且 $u-m\geqslant 2$.

证明 如果 $m=1$, 由引理 14.5.26, 定理成立. 根据引理 14.5.28 和定理 14.5.29 可设 $m\geqslant 2, n\geqslant 8$, 且 $G'=\langle g\rangle$. 令 $\overline{G}=G/\langle g^{2^{m-1}}\rangle$, 则 $|\overline{G}'|=2^{m-1}$. 由 [26] 中的命题 1.23, $G/\langle g^2\rangle$ 为非 Dedekind 群. 从而 $\overline{G}$ 为非 Dedekind 群. 由归纳假设, $\overline{G}$ 为定理中所设的群, 仅参数不同而已.

因为 G' 循环, 得到 $a^{2^u}=g^{2^{m-1}}$. 计算可知 $[b^{2^v},a]=a^{k2^{u+1-m+v}}$, 其中 $2\nmid k$. 从而 $v\geqslant m\geqslant 2$. 若 $[b,a]=a^{2^{u+1-m}+2^u}$, 令 $b_1=b^{1+2^{m-1}}$. 则 $[b_1,a]=a^{2^{u+1-m}}$. 于是可设 $[b,a]=a^{2^{u+1-m}}$. 同理可设 $[x_i,a]=1$. 若 $b^{2^v}=a^{2^u}$, 令 $b_2=ba^{2^{u-v}}$. 则 $b_2^{2^v}=1$. 故设 $b^{2^v}=1$. 同理可设 $x_i^{2^{e_i}}=1$. 这推出 $|\Omega_1(G)|\geqslant 16$. 由引理 14.5.19 得 $[b,x_i]=1$. 设 $A=\langle b,x_i\rangle$, $B=\langle b,x_j\rangle$. 由于 G 是 2 平衡 2 群, 则 $[x_i,x_j]=1$. 由此可得 G 为定理中的群. □

由定理 14.5.29 和定理 14.5.30, 我们可得到下面的结论.

推论 14.5.31 设 G 是 2 平衡 2 群, $|G|=2^n$, $d(G)\geqslant 4$, 且 $n\geqslant 7$. 则 G 是模群, 且 $G'\leqslant\langle x\rangle$, 其中 x 是 G 中满足 $o(x)=\exp(G)$ 的任意元素.

14.6 有限 p 群的特征标的核

设 G 是有限群, G 的所有非线性不可约特征标的核组成的集合记为 $\mathrm{Kern}(G)$. 由于每个正规子群总是 G 的一些不可约特征标的核的交, 因而 $\mathrm{Kern}(G)$ 对 G 的结构有着重要的影响. 钱国华等在文献 [183] 分类了 $\mathrm{Kern}(G)$ 在包含意义下恰为一条链的有限 p 群. 本节介绍他们的工作.

以下 $\mathrm{Irr}(G)$ 表示有限群 G 的不可约复特征标的集合且 $\mathrm{cd}(G):=\{\chi(1)\mid\chi\in\mathrm{Irr}(G)\}$.

引理 14.6.1 设 G 是有限 p 群且 $c(G)=3$. 若 $G_3=Z(G)\bigcap G_2, |G_3|=p$ 且 G_2/G_3 循环, 则 G/G_3 有交换极大子群. 进一步, $\mathrm{cd}(G/G_3)=\{1,p\}$.

证明 取 $y_1 \in G_2 \backslash G_3$ 使得 $G_2 = \langle y_1 \rangle G_3$ 以及 $y_2 \in G_2 \backslash G_3$. 由 [90] 中的推论 2.24 可知, $|C_{G/G_3}(y_2 G_3)| \leqslant |C_G(y_2)|$. 因而

$$p^{-1}|G| = |C_{G/G_3}(y_2 G_3)| \leqslant |C_G(y_2)| \leqslant p^{-1}|G|$$

且

$$C_G(y_1) = C_G(G_2) \leqslant C_G(y_2).$$

故对任意 $y_2 \in G_2 \backslash G_3$, 有 $C_G(y_2) = C_G(G_2)$ 且阶为 $p^{-1}|G|$. 取 $x \in G \backslash C_G(G_2)$, 则 $C_G(x) \bigcap G_2 = G_3$. 由于 $G_2/G_3 \leqslant Z(G/G_3)$, 故有

$$C_G(x)G_2/G_3 = C_G(x)/G_3 \times G_2/G_3.$$

注意到

$$|C_G(x)/G_3| = p^{-1}|C_G(x)| \geqslant p^{-1}|G/G_2|, \quad C_G(x)/G_3 \cong C_G(x)G_2/G_2 \leqslant G/G_2 \text{ 交换}.$$

因此 $C_G(x)G_2/G_3$ 交换且阶至少为

$$p^{-1}|G/G_2||G_2/G_3| = p^{-1}|G/G_3|.$$

由于 $|G/G_3|$ 非交换, 故 $|G/G_3 : C_G(x)G_2/G_3| = p$. 由 [90] 中的定理 12.11 可得, $\mathrm{cd}(G/G_3) = \{1, p\}$. □

设 G 是非交换 p 群, 易见 $c(G) \leqslant 1 + \log_p |G'|$. 由引理 14.6.1 可得下面的结论.

推论 14.6.2 设 G 是有限 p 群且 $c(G) \geqslant 3$. 则 G 是极大类的当且仅当 $c(G) = 1 + \log_p |G'|$ 且 G/G_3 为超特殊 p 群.

引理 14.6.3 设 G 是有限非交换群, K 是 $\mathrm{Kern}(G)$ 中所有子群的交, 则 $K = 1$.

证明 由 [90] 中的引理 2.21, 推论 2.23 可知, $K \bigcap G' = 1$. 假设 $K > 1$. 设 λ 为 K 的不可约的非主特征标, χ 为 λ^G 的任意一个不可约成分, 则 $\mathrm{Ker}\,\chi \ngeqslant K$. 因此 χ 为线性的且 χ 为 λ 的一个扩张. 取非线性特征标 $\psi_0 \in \mathrm{Irr}(G/K)$, 由 [90] 中的推论 6.17 可知, $\chi\psi_0 \in \mathrm{Irr}(G)$ 非线性且 $\mathrm{Ker}\,(\chi\psi_0) \ngeqslant K$, 矛盾. □

定义 14.6.4 设 K 为有限群 G 的正规子群. 若对 G 的任意正规子群 T 总有 $T \geqslant K$ 或 $T < K$, 则称 K 为 G 的重子群.

定理 14.6.5 设 G 是有限非交换 p 群, 则下列陈述两两等价.

(1) $\mathrm{Kern}(G)$ 在包含意义下是一条链.

(2) G 的所有包含在 G' 中的正规子群均为 G 的重子群.

(3) 若 N 为 G 的真包含于 G' 的正规子群, 则 $N \in \mathrm{Kern}(G)$.

(4) G 是下列群之一:

(4.1) G' 是 G 的唯一极小正规子群;

(4.2) G 是极大类群.

证明 (1) ⇒ (2): 假设 Kern(G) 在包含意义下是一条链. 设 $K\lhd G$ 且 $K\leqslant G'$. 任取 G 的正规子群 T, 考虑商群 $G/(T\bigcap K)$. 若 $G/(T\bigcap K)$ 交换, 则 $T\geqslant T\bigcap K\geqslant G'\geqslant K$. 下设 $G/(T\bigcap K)$ 非交换. 设 $\chi_1,\cdots,\chi_s$ 为 G 的所有满足 $T\bigcap K\leqslant \mathrm{Ker}\ \chi_i$ 的非线性不可约特征标. 显然, 这些 χ_i 恰为 $G/(T\bigcap K)$ 的所有非线性不可约特征标. 由引理 14.6.3 可知, $T\bigcap K=\mathrm{Ker}\ \chi_1\bigcap\cdots\bigcap \mathrm{Ker}\ \chi_s$. 由题设条件可设 $\mathrm{Ker}\ \chi_1\leqslant \mathrm{Ker}\ \chi_2\leqslant\cdots\leqslant \mathrm{Ker}\ \chi_s$, 因此 $G/(T\bigcap K)$ 有一个忠实的不可约特征标 χ_1. 由 [90] 中的引理 2.27 可知, $G/(T\bigcap K)$ 的中心循环. 假设 $T/(T\bigcap K)$ 与 $K/(T\bigcap K)$ 均不为 1. 由于 $G/(T\bigcap K)$ 为 p 群, 故

$$Z(G/(T{\textstyle\bigcap}K)){\textstyle\bigcap}T/(T{\textstyle\bigcap}K) \quad 与 \quad Z(G/(T{\textstyle\bigcap}K)){\textstyle\bigcap}K/(T{\textstyle\bigcap}K)$$

均不为 1. 进而 $Z(G/(T\bigcap K))$ 非循环, 矛盾. 因而, 必有 $T/(T\bigcap K)=1$ 或 $K/(T\bigcap K)=1$, 进一步, $T\leqslant K$ 或 $K\leqslant T$. 因此, G 的每个包含于 G' 的正规子群 K 均为 G 的重子群.

(2) ⇒ (4). 首先证明: 若 $N\lhd G$ 且 $N\leqslant G'$, 则 G/N 满足假设 (2). 设 K/N 与 T/N 为 G/N 的正规子群且 $K/N\leqslant (G/N)'=G'/N$. 则 K, T 为 G 的正规子群且 $K\leqslant G'$. 由于 K 是 G 的重子群, 故 $K\leqslant T$ 或 $K\geqslant T$. 进而有 $K/N\leqslant T/N$ 或 $K/N\geqslant T/N$. 因而 K/N 是 G/N 的重子群.

设 $|G'|=p$, 由于 G' 为 G 的重子群, 则 G' 为 G 的唯一的极小正规子群, 此时 G 为 (4.1) 型群.

下设 $|G'|\geqslant p^2$. 下证 G 是极大类 p 群. 记 $c(G)=n$.

断言 (Ⅰ): G_i/G_{i+1} 循环, 其中 $i=2,\cdots,n$.

由于 G/G_n 满足题设条件, 由归纳假设可知, 对于 $i=2,\cdots,n-1$, 有 G_i/G_{i+1} 循环. 由于 $G_n\leqslant Z(G)$, 故 G_n 的所有子群均正规, 因而是 G 的重子群. 由定义可知, G_n 的所有子群在包含意义下构成一条链, 因而 G_n 循环.

断言 (Ⅱ): 若 T 为 G 的交换正规子群且 $T\bigcap G_2$ 为阶至少为 p^2 的循环群, 则 T 循环.

考虑 $\Omega_1(T)=\langle x\in T\mid x^p=1\rangle$. 由于 $\Omega_1(T)$ 为 T 的特征子群, 故 $\Omega_1(T)\lhd G$. 由 $\Omega_1(T)$ 初等交换以及 $G_2\bigcap T$ 为阶至少为 p^2 的循环群可知, $\Omega_1(T)<G_2\bigcap T$. 因而 $\Omega_1(T)$ 为 p 阶循环群, 且 T 循环.

断言 (Ⅲ): $|G_2/G_3|=p$.

假设 $|G_2/G_3|\geqslant p^2$. 由归纳法, 我们可设 $G_3=1$. 由断言 (Ⅰ) 可知, G_2 循环. 任取 $x\in G\setminus G_2$, 由于 $G_2=G'\leqslant Z(G)$, 故 $\langle x\rangle G_2$ 为 G 的交换正规子群. 由断言 (Ⅱ) 可知, $\langle x\rangle G_2$ 循环. 因而, G_2 外的任一元素的阶至少为 p^3, 也即 G 只含一个 p 阶子群. 于是 G 为循环群或为广义四元数群. 由于 G 非交换, 且广义四元数群至少有两个 4 阶循环群, 故推出矛盾.

断言 (IV): 若 $|G_2| = p^2$, 则 G 是极大类的.

由断言 (III) 可知, $|G_2/G_3| = |G_3| = p$. 由引理 14.6.1 可知, $\mathrm{cd}(G/G_3) = \{1, p\}$. 设 $Z/G_3 = Z(G/G_3)$, 由于 G/G_3 为 (4.1) 型群, 由 [90] 中的引理 12.3 可知, $|G : Z| = p^2$ 且 Z/G_3 循环.

假设 $Z > G_2$ 且 Z 非循环. 由于 Z 交换, 故可设 $Z = A \times G_3$, 其中 $A \cong Z/G_3$. 令 $W = \langle g^p \mid g \in Z\rangle$, 则 W 为 Z 的特征子群, 进而 $W \lhd G$. 由于 $1 < W < A$, 故 $W \not\geqslant G_3$ 且 $W \not\leqslant G_3$. 这与 G_3 是 G 的重子群矛盾.

假设 $Z > G_2$ 且 Z 循环. 易见 $G_3 = Z(G), Z/Z(G) = Z(G/Z(G))$. 由 [89] 中的III, 定理 7.7 可知, $p = 2$ 且 G 有指数为 2 的循环子群. 因而 $|G/G_2| = 4$ 或 $|G_2| = 2$(见 [89] 中的 I , 定理 14.9), 矛盾. 因此, $Z = G_2$, G 为极大类的.

断言 (V): G 为极大类的.

取 $E \lhd G$ 满足 $|G_2/E| = p^2$. 由于 G/E 满足题设条件, 由断言 (IV) 可知, G/E 是极大类的. 特别地, G/G_2 为 p^2 阶初等交换 p 群. 若 $p = 2$, 由 [89] 中的III, 定理 11.9 可知, G 为极大类的. 下设 $p > 2$. 由断言 (III) 和断言 (IV) 可知, G/G_n 为极大类的. 特别地, 对 $i = 2, \cdots, n-1$, 有 $|G_i/G_{i+1}| = p$. 只需证明: $|G_n| = p$. 假设 $|G_n| \geqslant p^2$. 由于 G_n 循环, 故存在满足 $2 \leqslant s \leqslant n$ 且 G_s 循环的最小正整数 s. 设 T/G_s 为 G 的任一主因子.

假设存在主因子 T/G_s 满足 T 非交换. 则 T 非交换且 T 有一个指数为 p 的循环子群 G_s. 由 [89] 中的III, 引理 8.7 可知, T 有唯一的非循环的极大子群 A. 因而 A 为 T 的特征子群且 $A \lhd G$. 显然, $A \not\geqslant G_s$ 且 $A \not\leqslant G_s$. 这与 G_s 为 G 的重子群矛盾.

设对任意 G 的主因子 T/G_s 均有 T 交换. 由断言 (III) 可知 T 交换. 假设 $s \geqslant 3$. 由于 $|G_{s-1}/G_s| = p$, 故可取 $T = G_{s-1}$. 于是 G_{s-1} 循环, 这与 s 的取法矛盾. 因而 $G_2 = G_s$. 任取 $x \notin G_2$. 由于 G/G_2 初等交换, 故可取 $T = \langle x\rangle G_2$. 由于 T 循环, 故 x 的阶至少是 p^3. 因而 G 有唯一的 p^2 阶子群, 这与 [89] 中的III, 定理 3.8 矛盾. 因而 $|G_n| = p$, 且 G 为极大类的.

(4) $\Rightarrow$ (1) 且 (4) $\Rightarrow$ (3): 设 G 是满足 (4.1) 或 (4.2) 的有限 p 群, 则对任意 $p^i = p^0, p^1, \cdots, p^t = |G'|$, G' 有唯一的 p^i 阶 G 的正规子群 N_i. 于是, $1 = N_0 < N_1 < \cdots < N_t = G'$.

任取 $K \in \mathrm{Kern}(G)$, 选取 G 的满足 G/E 非交换且 $E \geqslant K$ 的极大正规子群 E. 由 [90] 中的引理 12.3 可知, $G'E/E$ 为 p 阶循环群, 因而 $|G'/(G' \bigcap E)| = p$. 于是 $G' \bigcap E = N_{t-1}$. 由于 G/N_{t-1} 为 (4.1) 型群, G'/N_{t-1} 为 G/N_{t-1} 的唯一极小正规子群. 于是 $E/N_{t-1} = 1$, $E = N_{t-1} = G' \bigcap E$, 且 $K \leqslant E < G'$. 因此, $\mathrm{Kern}(G)$ 是集合 $\{N_i \mid 0 \leqslant i \leqslant t-1\}$ 的子集, 且 $\mathrm{Kern}(G)$ 在包含意义下是一条链, (1) 成立.

由引理 14.6.3 可知,

$$N_i = \bigcap\{\text{Ker } \chi \mid \chi \in \text{Irr}(G), N_i \leqslant \text{Ker } \chi, \chi(1) > 1\}.$$

由于 Kern(G) 在包含意义下是一条链, 故存在 G 的非线性不可约特征标 χ, 使得 $N_i = \text{Ker}\chi$, (3) 成立.

(3) $\Rightarrow$ (2): 设 E, K 为 G 的正规子群且 $E \leqslant G'$, 则 $E \leqslant K$ 或 $E\bigcap K < E \leqslant G'$. 假设 $E\bigcap K < E \leqslant G'$, 则 $E\bigcap K \in \text{Kern}(G)$. 由 [90] 中的引理 2.27 可知, $Z(G/(E\bigcap K))$ 循环. 类似于 (1) $\Rightarrow$ (2) 的证明, 我们可得 $K = E\bigcap K$, 即 $K \leqslant E$. 因此 G 的包含在 G' 中的正规子群均为 G 的重子群, (2) 成立. □

注 14.6.6 假设 G 是有限群但不是 p 群. 若 G 的包含在 G' 中的正规子群均为 G 的重子群, 则 Kern(G) 在包含意义下是一条链. 但反过来不成立.

证明 设 $1 = N_0, N_1, \cdots, N_s = G'$ 为 G 的包含在 G' 中的所有正规子群且均为 G 的重子群, 由重子群的定义可设 $1 = N_0 < N_1 < \cdots < N_s = G'$. 设 $K \in \text{Kern}(G)$. 由 G' 为 G 的重子群可得 $G' > K$ 或 $G' < K$. 由 G/K 非交换得 $G' > K$. 于是 Kern(G) 为集合 $\{N_i \mid 1 \leqslant i \leqslant s-1\}$ 的子集. 因而 Kern(G) 在包含意义下是一条链.

设 $G = H \times U$, 其中 H 为 8 阶非交换群, U 为 3 阶循环群, 则 Kern$(G) = \{1, U\}$. 由于 $H' \nleqslant U$ 且 $H' \ngeqslant U$, 故 $G' = H'$ 不是 G 的重子群. □

注 14.6.7 设 G 是有限群但不是 p 群. 若 Kern(G) 在包含意义下是一条链, 则对任意的真包含在 G' 中的 G 的正规子群 N 有 $N \in \text{Kern}(G)$. 但反过来不成立.

证明 设 Kern(G) 在包含意义下是一条链, $N \trianglelefteq G$ 且 $N < G'$. 由引理 14.6.3 可知,

$$N = \{\text{Ker } \chi \mid \chi \in \text{Irr}(G), N \leqslant \text{Ker } \chi, \chi(1) > 1\},$$

因而存在非线性不可约特征标 χ 使得 $N = \text{Ker } \chi$.

下面证明逆命题不成立. 设 $G = H \times U$, 其中 $H \cong \text{Q}_{16}$, $U \cong \text{C}_3$, 则 $H' = G'$ 且 $1, Z(H)$ 是 G 的包含在 G' 中的所有正规子群. 设 χ_1, χ_2 分别为 H 的 2 次和 4 次不可约特征标, σ 为 U 的忠实的线性特征标, 则 $\chi_1 \times \sigma$ 和 $\chi_2 \times \sigma$ 为 G 的非线性不可约特征标, 且它们的核分别为 $Z(H)$ 和 1. 但 U 是不可约特征标 $\chi_1 \times 1_U$ 的核, 其中 1_U 为 U 的主特征标. 因此 Kern(G) 在包含意义下不是一条链. □

推论 14.6.8 设 G 为非交换幂零群, 若 Kern(G) 在包含意义下是一条链, 则 G 或者为定理 14.6.5中所述的群, 或者 $G = P \times U$, 其中 P 为定理 14.6.5中的(4.1)型群, U 为素数幂阶循环 p' 群.

证明 设 $P \in \text{Syl}_p(G)$ 且 P 非交换. 则 $G = P \times U$, 其中 U 为幂零的 p' 群. 显然, Kern(G/U) 在包含意义下是一条链. 因此, P 是定理 14.6.5(4) 中所述的群之一.

假设 $G > P$. 设 χ 为 P 的非线性不可约特征标, λ 为 U 的线性特征标. 此时 $\psi_\lambda := \chi \times \lambda \in \mathrm{Irr}(G)$ 且 $\mathrm{Kern}\psi_\lambda = \mathrm{Kern}\chi \times \mathrm{Kern}\lambda$. 由于集合 $\{\mathrm{Kern}(\psi_\lambda) \mid \lambda \in \mathrm{Irr}(U), \lambda(1) = 1\}$ 中的子群构成一条链, 因而 $\{\mathrm{Kern}(\lambda) \mid \lambda \in \mathrm{Irr}(U), \lambda(1) = 1\}$ 在包含意义下也是一条链. 于是 U/U' 是素数幂阶循环群, 进而 U 也是素数幂阶循环群. 下面只需证明 P 是定理 14.6.5 中的 (4.1) 型群. 否则, P 是 (4.2) 型群. 此时存在 P 的非线性不可约特征标 χ_1, χ_2 使得 $\mathrm{Kern}\chi_1 = 1$, $P_1 := \mathrm{Kern}\chi_2 > 1$. 因而 $P_1 = \mathrm{Kern}(\chi_2 \times \lambda)$, 其中 λ 为 U 的忠实的线性特征标, 且 $U = \mathrm{Kern}(\chi_1 \times 1_U)$. 于是 P_1, U 均属于 $\mathrm{Kern}(G)$, 进而 $\mathrm{Kern}(G)$ 在包含意义下不是一条链, 矛盾. □

14.7　自同构群相同的 2 群的例子

众所周知, 两个不同的群可能有相同的自同构群, 例如, $\mathrm{Aut}(\mathrm{C}_3) \cong \mathrm{Aut}(\mathrm{C}_4) \cong \mathrm{C}_2$ 和 $\mathrm{Aut}(\mathrm{C}_4 \times \mathrm{C}_2) \cong \mathrm{Aut}(\mathrm{D}_8) \cong \mathrm{D}_8$. 其中 C_n 和 D_n 分别表示 n 阶循环群和 n 阶二面体群. 但是对一个给定的素数 p, 还不知道是否存在两个不同阶的非平凡 p 群具有相同的自同构群. 进一步地, Berkovich 提出了下列问题: 是否存在一个 p 群 G 及其真子群 H 使得 $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$? 见 [26] 中的 Problem 211. 该问题也在 Khukhro 和 Mazurov 的书 [112] 中作为问题 15.27 提出. 对于 $p = 2$, 李天则在文献 [132] 中构造了一个简单例子对这个问题给出正面的回答.

用 C_2^n 表示 2^n 阶的初等交换 2 群. 令 $C = \langle x_1 \rangle = \mathrm{C}_4$ 且 $E = \langle x_2, x_4, x_5 \rangle = \mathrm{C}_2^3$. E 的生成元下标在后续中是清楚的.

设 $G = E \rtimes C = \mathrm{C}_2^3 \rtimes \mathrm{C}_4$, 即 E 和 C 在同态 φ 之下的半直积, 其中 φ: $C \to \mathrm{Aut}(E)$ 定义为

$$\varphi(x_1)(x_2) = x_2 x_4, \quad \varphi(x_1)(x_4) = x_4 x_5, \quad \varphi(x_1)(x_5) = x_5.$$

设 $x_3 = x_1^2$. 显然,

$$[x_3, x_2] = x_5, \quad [x_3, x_4] = 1, \quad [x_3, x_5] = 1.$$

设 $H = \langle x_2, x_3, x_4, x_5 \rangle$. 显然 $H = \langle x_2, x_3 \rangle \times \langle x_4 \rangle = \mathrm{D}_8 \times \langle x_4 \rangle$.

下面, 我们将证明 $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$. 为此, 先需要 G 和 H 的特征子群的一些信息.

引理 14.7.1　*构造的群 G 和 H 具有下列的性质.*

(1) $H' = \langle x_5 \rangle$ 且 $Z(H) = \langle x_4, x_5 \rangle$;

(2) $Z(G) = \langle x_5 \rangle$ 且 $G' = \langle x_4 \rangle \times \langle x_5 \rangle$;

(3) $\Omega_1(G) = H$;

(4) $\Phi(G) = \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle$ 且 $G/\Phi(G) = \langle \bar{x}_1 \rangle \times \langle \bar{x}_2 \rangle \cong \mathrm{C}_2 \times \mathrm{C}_2$.

证明 G 的任意元素可以唯一表示为 $x_1^k y$ 的形式, 其中 $0 \leqslant k \leqslant 3$ 且 $y \in E$. 计算可得 $G \setminus H$ 中的元素都为 4 阶. 因此 (3) 成立. 因为 G 是一个 2 群, 故 $\Phi(G) = G'\mho_1(G)$. 其他的证明可以直接得到. □

现在我们证明如下定理.

定理 14.7.2 $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$.

证明 先决定 $\mathrm{Aut}(H)$. 注意到 H 的任意元都可唯一表示为 $x_2^{a_2}(x_2x_3)^{a_3}x_4^{a_4}x_5^{a_5}$ 的形式, 其中 $a_2, a_3, a_4, a_5 \in \{0, 1\}$. 令 $\varphi \in \mathrm{Aut}(H)$. 考虑 $\varphi(x_i)$, $i = 2, 3, 4, 5$. 由引理 14.7.1(1) 可知

$$\varphi(x_5) = x_5, \quad \varphi(x_4) = x_4x_5^a, \quad \varphi(x_3) = x_2(x_2x_3)^b x_4^c x_5^d, \quad \varphi(x_2) = x_2(x_2x_3)^e x_4^f x_5^g,$$

其中 $a, b, c, d, e, f, g \in \{0, 1\}$. 因为 x_2x_3 的阶为 4, 故有 $b+e = 1$. 另一方面, 可知满足上述条件的任意一组 a, b, c, d, e, f, g 决定了 H 的一个自同构. 于是 $|\mathrm{Aut}(H)| = 2^6$.

如下定义 $\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6 \in \mathrm{Aut}(H)$:

$$\varphi_1 : \begin{cases} x_2 \to x_2, \\ x_3 \to x_3, \\ x_4 \to x_4x_5, \end{cases} \qquad \varphi_2 : \begin{cases} x_2 \to x_3, \\ x_3 \to x_2, \\ x_4 \to x_4, \end{cases} \qquad \varphi_3 : \begin{cases} x_2 \to x_2x_4, \\ x_3 \to x_3, \\ x_4 \to x_4, \end{cases}$$

$$\varphi_4 : \begin{cases} x_2 \to x_2x_5, \\ x_3 \to x_3, \\ x_4 \to x_4, \end{cases} \qquad \varphi_5 : \begin{cases} x_2 \to x_2, \\ x_3 \to x_3x_4, \\ x_4 \to x_4, \end{cases} \qquad \varphi_6 : \begin{cases} x_2 \to x_2, \\ x_3 \to x_3x_5, \\ x_4 \to x_4. \end{cases}$$

显然上述自同构都是 2 阶的.

注意到有一个自然同态 $\mathrm{Aut}(H) \to \mathrm{Aut}(Z(H)) \cong \mathrm{GL}(2, 2)$. 令 K 为这个自然同态的核. 则 $\mathrm{Aut}(H) = K \rtimes \langle \varphi_1 \rangle$. 直接计算可得 $\varphi_3, \varphi_4, \varphi_5, \varphi_6$ 之间可交换. 此外

$$\varphi_3^{\varphi_2} = \varphi_5, \quad \varphi_5^{\varphi_2} = \varphi_3, \quad \varphi_4^{\varphi_2} = \varphi_6, \quad \varphi_6^{\varphi_2} = \varphi_4.$$

因为 $|K| = 2^5$, 所以

$$K = \langle \varphi_3, \varphi_4, \varphi_5, \varphi_6 \rangle \rtimes \langle \varphi_2 \rangle \cong \mathrm{C}_2^4 \rtimes \mathrm{C}_2.$$

并且, φ_1 如下作用于 K:

$$\varphi_3^{\varphi_1} = \varphi_3\varphi_4, \quad \varphi_5^{\varphi_1} = \varphi_5\varphi_6, \quad \varphi_4^{\varphi_1} = \varphi_4, \quad \varphi_6^{\varphi_1} = \varphi_6, \quad \varphi_2^{\varphi_1} = \varphi_2.$$

现在考虑 $\mathrm{Aut}(G)$. 注意到 G 的任意元都可唯一表示为 $x_1^{b_1}x_2^{b_2}x_3^{b_3}x_4^{b_4}x_5^{b_5}$ 的形式, 其中 $b_1, b_2, b_3, b_4, b_5 \in \{0, 1\}$. 令 $\theta \in \mathrm{Aut}(G)$. 由引理 14.7.1 可知

$$\theta(x_5) = x_5, \quad \theta(x_4) = x_4x_5^a, \quad \theta(x_3) = x_3x_4^b x_5^c,$$

$$\theta(x_2)=x_2x_3^dx_4^ex_5^f,\quad \theta(x_1)=x_1x_2^gx_3^hx_4^ix_5^j,$$

其中 $a,b,c,d,e,f,g,h,i,j\in\{0,1\}$. 因为

$$\theta(x_2)^2=1,\quad \theta(x_1)^2=\theta(x_3)\quad 且\quad [\theta(x_1),\theta(x_2)]=\theta(x_4),$$

我们也有 $d=0$, $b\equiv g, c\equiv i+gh$ 且 $a\equiv e+h(\bmod 2)$. 另一方面, 可知满足上述条件的任意一组 a,b,c,d,e,f,g,h,i,j 决定了 G 的一个自同构. 于是 $|\mathrm{Aut}(G)|=|\mathrm{Aut}(H)|=2^6$.

下面决定 $\theta_1,\theta_2,\theta_3,\theta_4,\theta_5,\theta_6,\theta_2'\in\mathrm{Aut}(H)$.

$$\theta_1:\begin{cases}x_1\to x_1x_2,\\ x_2\to x_2,\\ x_3\to x_3x_4,\\ x_4\to x_4,\end{cases}\quad \theta_2:\begin{cases}x_1\to x_1x_3x_5,\\ x_2\to x_2x_4x_5,\\ x_3\to x_3,\\ x_4\to x_4,\end{cases}\quad \theta_3:\begin{cases}x_1\to x_1x_3,\\ x_2\to x_2,\\ x_3\to x_3,\\ x_4\to x_4x_5,\end{cases}\quad \theta_4:\begin{cases}x_1\to x_1x_4,\\ x_2\to x_2,\\ x_3\to x_3x_5,\\ x_4\to x_4,\end{cases}$$

$$\theta_5:\begin{cases}x_1\to x_1x_5,\\ x_2\to x_2,\\ x_3\to x_3,\\ x_4\to x_4,\end{cases}\quad \theta_6:\begin{cases}x_1\to x_1,\\ x_2\to x_2x_5,\\ x_3\to x_3,\\ x_4\to x_4,\end{cases}\quad \theta_2':\begin{cases}x_1\to x_1,\\ x_2\to x_2x_4,\\ x_3\to x_3,\\ x_4\to x_4x_5.\end{cases}$$

上述自同构除了 θ_2' 都是 2 阶的. θ_2' 的阶为 4 且 $\theta_2=\theta_5\theta_3\theta_2'$.

类似地, 有一个自然同态 $\mathrm{Aut}(G)\to\mathrm{Aut}(G/\Phi(G))\cong\mathrm{GL}(2,2)$. 令 L 为这个自然同态的核. 则

$$\mathrm{Aut}(G)=L\rtimes\langle\theta_1\rangle,\quad L=\langle\theta_3,\theta_4,\theta_5,\theta_6\rangle\rtimes\langle\theta_2\rangle\cong\mathrm{C}_2^4\rtimes\mathrm{C}_2,$$

其中

$$\theta_3^{\theta_2}=\theta_3\theta_6,\quad \theta_4^{\theta_2}=\theta_4\theta_5,\quad \theta_5^{\theta_2}=\theta_5,\quad \theta_6^{\theta_2}=\theta_6,$$

并且 θ_1 如下作用于 L:

$$\theta_3^{\theta_1}=\theta_3\theta_4,\quad \theta_4^{\theta_1}=\theta_4,\quad \theta_5^{\theta_1}=\theta_5,\quad \theta_6^{\theta_1}=\theta_6\theta_5,\quad \theta_2^{\theta_1}=\theta_2.$$

定义 $\psi:\mathrm{Aut}(G)\to\mathrm{Aut}(H)$ 为 $\psi(\theta_i)=\varphi_i$, 其中 $1\leqslant i\leqslant 4$, $\psi(\theta_5)=\varphi_4\varphi_6$ 且 $\psi(\theta_6)=\varphi_3\varphi_5$. 由以上的讨论易得 ψ 是一个同构映射. □

注 14.7.3　*在计算代数系统 GAP [216] 中的小群库中, $G\cong\mathrm{SmallGroup}(32,6)$, $H\cong\mathrm{SmallGroup}(16,11)$ 且 $\mathrm{Aut}(G)\cong\mathrm{Aut}(H)\cong\mathrm{SmallGroup}(64,138)$. 在 Hall-Senior 群表 [76] 中, H 为 16 阶群中的 6 号群, G 为 32 阶群中的 46 号群且 $\mathrm{Aut}(G)\cong\mathrm{Aut}(H)$ 为 64 阶群中的 259 号群.*

读者欲了解 GAP 的有关知识, 可参考书 [248].

14.8 极大交换子群为软的 p 群

对于有限 p 群, Héthelyi 在文献 [83] 引进了**软子群**的概念: 有限 p 群的子群 H 称为软的 (soft), 若 $C_G(H)=H$ 且 $|\mathrm{Aut}_G(H)|=p$. 该文建立了软子群的某些基本性质. Héthelyi 在文献 [84],[85] 中继续对具有一个软子群的有限 p 群进行研究, 得到了许多有趣的结果. 特别是他在文献 [85] 证明了: 一个有限 2 群的每个极大交换子群是软的当且仅当 $G/Z(G)$ 是二面体群. 作为该结果的推论, 他证明了: 若 G 是二元生成的具有交换极大子群的有限 2 群, 则 $G/Z(G)$ 是二面体群. 李世荣在文献 [129] 从极大类 p 群的观察出发, 引进了广义极大类 p 群概念: 有限 p 群 G 称为**广义极大类的**, 若 $c(G)=1+\log_p(|G'|)$. 他在该文中证明并推广了文献 [85] 的工作, 给出了一类广义极大类 p 群. 曲海鹏在短文 [187] 进一步推广了文献 [129] 的结果到有限 p 群. 下面的内容取自 [187].

引理 14.8.1 *设 G 为极大类群且 A 为 G 的交换极大子群. 若 H 为 G 的子群满足 $H\nleqslant A$ 且 $|H|\geqslant p^3$, 则 H 是极大类群.*

证明 对 $|G:H|$ 进行归纳. 若 $|G:H|=p$, 则由文献 [89] 中的III, 定理 14.11, 定理 14.22 可得结论成立. 若 $|G:H|>p$, 则取子群 K 满足 $|K:H|=p$. 由 $|G:K|<|G:H|$ 可得 K 是极大类群. 因此 H 是极大类群. □

引理 14.8.2 *设 A 为 G 的交换极大子群且 $d(G)=2$. 则 $G/Z(G)$ 是极大类群.*

证明 取 $b\in G\setminus A$ 且 $a\in A\setminus\Phi(G)$. 则 $G=\langle a,b\rangle$. 设 $c(G)=c$. 则

$$G_i=\langle[a,(i-1)b],G_{i+1}\rangle,\quad \text{其中}\quad 2\leqslant i\leqslant c.$$

首先, 我们断言 $|G_c|=p$ 且 $|G'|=p^{c-1}$. 因为 $G_c=\langle[a,(c-1)b]\rangle\leqslant Z(G)$, 故 $[a,(c-1)b]^p=[a,(c-2)b,b^p]=1$. 因此 $|G_c|=p$. 为了证明 $|G'|=p^{c-1}$, 我们对 $c(G)$ 进行归纳. 设 $c>2$. 由 A 的极大性可知 $G_c\leqslant A$. 因此 A/G_c 为 G/G_c 的交换极大子群且 $d(G/G_c)=2$. 由归纳假设可知

$$|G'/G_c|=|(G/G_c)'|=p^{c(G/G_c)-1}=p^{c-2}.$$

因此 $|G'|=p^{c-1}$.

其次, 由定理 1.7.6 可知 $|G|=p|G'||Z(G)|$. 则 $|G/Z(G)|=p|G'|=p^c$. 因为 $c(G/Z(G))=c-1$, 故 $G/Z(G)$ 是极大类群. □

定理 14.8.3 *令 G 为非交换 p 群. 则下列陈述是等价的:*

(1) 若 H 为 G 的交换子群, 则 $|N_G(H)/C_G(H)|\leqslant p$;

(2) G 的极大交换子群是软的;

(3) G 有交换极大子群, 且 $G/Z(G)$ 是极大类群.

证明　(1) ⇒ (2): 显然成立.

(2) ⇒ (3): 令 A 为 G 的极大交换的正规子群. 众所周知, A 也为 G 的极大交换子群. 由假设可知 $|G/A| = |N_G(A)/C_G(A)| = p$. 因此 A 为 G 的交换极大子群.

令 $G = A\langle x\rangle$ 且 $B = Z(G)\langle x\rangle$. 因为

$$C_G(B) = C_G(x) = C_G(x)\bigcap G = C_G(x)\bigcap(A\langle x\rangle) = (C_G(x)\bigcap A)\langle x\rangle = Z(G)\langle x\rangle = B,$$

故 B 为 G 的极大交换子群. 由假设可得 B 在 G 中是软的.

令 $M = \Phi(G)B$. 因为 $B \subseteq M$ 且 $M \trianglelefteq G$, 由文献 [83] 可得 M 是唯一包含 B 的极大子群. 取 $y \in G\backslash M$, 令 $K = \langle x, y\rangle$. 则

$$G = \langle M, y\rangle = \langle B, y\rangle = \langle Z(G), x, y\rangle = Z(G)K.$$

因此 $G/Z(G) \cong K/K\bigcap Z(G) = K/Z(K)$. 已知 $d(K) = 2$ 且 $A\bigcap K$ 为 K 的交换极大子群. 由引理 14.8.2 可得 (3) 成立.

(3) ⇒ (1): 若否, 令 G 为极小的反例且 A_1 为 G 的满足 $|N_G(A_1)/C_G(A_1)| \geqslant p^2$ 的最大阶交换子群. 取 $N_G(A_1)$ 的极大交换正规子群 B, 其中 $B \geqslant A_1$. 易得 B 为 G 的极大交换子群. 因为 $C_G(A_1) \geqslant B = C_G(B)$ 且 $N_G(A_1) \leqslant N_G(B)$, 故 $|N_G(B)/C_G(B)| \geqslant p^2$. 由 A_1 的极大性可得 $B = A_1$, 即 A_1 为 G 的极大交换子群. 因此 $Z(G) \leqslant A_1$. 此外, $N := N_G(A_1)$ 非交换. 令 A 为 G 的交换极大子群. 则 $A\bigcap N$ 为 N 的交换极大子群. 因为 $A_1/Z(G) \nleqslant A/Z(G)$, 故 $|N/Z(G)| \geqslant p^2|A_1/Z(G)| \geqslant p^3$. 由引理 14.8.1 可得 $N/Z(G)$ 是极大类群.

令 $N = (A\bigcap N)\langle x\rangle$. 则 $G = A\langle x\rangle$, 从而

$$Z(N) = C_{A\bigcap N}(x) \leqslant C_A(x) = Z(G).$$

进而 $Z(N) = Z(G)$. 因此 $N/Z(N)$ 是极大类群. 注意到

$$|N_N(A_1)/A_1| = |N_G(A_1)/A_1| \geqslant p^2.$$

由 G 的极小性可得 $G = N$ 且 $A_1 \trianglelefteq G$. 因此

$$A_1/Z(G) \trianglelefteq G/Z(G), \quad |G/Z(G)/A_1/Z(G)| = |G/A_1| \geqslant |N_G(A_1)/A_1| \geqslant p^2.$$

因为 $G/Z(G)$ 是极大类群, 故 $G/Z(G)$ 的非极大的真正规子群包含于 $\Phi(G/Z(G))$. 所以 $A_1/Z(G) \leqslant A/Z(G)$, 矛盾. □

命题 14.8.4　令 G 为定理 14.8.3(3)中的群. 设 $c(G) = c$. 若 $p = 2$, 则 $G/Z(G) \cong \mathrm{D}_{2^c}$.

证明　令 $G=\langle a,b,Z(G)\rangle$ 且 $H=\langle a,b\rangle$. 则 $H/Z(H)=H/H\bigcap Z(G)\cong G/Z(G)$. 不失一般性可设 $d(G)=2$. 则有如下事实: 若 t 为整数, 则不存在 $\bar{x},\bar{y}\in G/Z(G)$ 使得 $G/Z(G)=\langle\bar{x},\bar{y}\rangle$ 且 $1\neq\bar{x}^t\in\langle\bar{y}\rangle$. 若否. 由 $1\neq\bar{x}^t$ 可得 $x^t\notin Z(G)$. 但易算出 $[x^t,x]=1=[x^t,y]$, 矛盾. 若 $p=2$, 则极大类 2 群只有二面体群, 半二面体群和广义四元数群. 以文献 [89] 中的III, 定理 11.9b 为例. 令 $t=2$. 则由上面的事实可得 $G/Z(G)$ 为二面体群. □

注 14.8.5　定理 14.8.3 和命题 14.8.4 推广了文献 [129] 中的定理 3.1 的主要结论.

14.9　有限 p 群的子群交

众所周知, Frattini 子群在有限群的研究中起着极其重要的作用. 本节考虑有限 p 群 G 的三类子群的交对 G 的结构的影响. 一个是 G 的所有 p^k 阶子群的交, 记为 $\mathrm{I}_k(G)$. 另一个是 G 的所有 $\mathcal{A}_1$ 子群的交, 记为 $\mathrm{I}_{\mathcal{A}_1}(G)$. 再一个是 G 的所有非内交换的极大子群的交, 记为 $\Phi_{N\mathcal{A}_1M}(G)$. 显然, 它们都是 G 的特征子群. Golovanov 在文献 [68] 分类了 $\mathrm{I}_2(G)=2$ 的有限 2 群. 安立坚等在文献 [4] 分类了 $\mathrm{I}_3(G)=4$ 的有限 2 群. 对于 $2\leqslant k\leqslant n-1$, 张勤海等在文献 [276] 分类了 $\mathrm{I}_k(G)\cong\mathrm{C}_{p^{k-1}}$ 的有限 p 群. 张丽华在文献 [266],[267] 分别分类了 $|\mathrm{I}_{\mathcal{A}_1}(G)|\leqslant p^{n-3}$ 的 p^n 阶群以及 $\Phi_{N\mathcal{A}_1M}(G)>\Phi(G)$ 的有限 p 群. 本节介绍这些结果.

14.9.1　$\mathrm{I}_k(G)\cong\mathrm{C}_{p^{k-1}}$ 的 p 群

设 G 是有限 p 群. 当 $p>2$ 且 $|G|=p^3$ 时, 易证: G 满足 $\mathrm{I}_2(G)\cong\mathrm{C}_p$ 当且仅当 G 是 $\mathrm{C}_{p^2}\times\mathrm{C}_p$, $\mathrm{M}_p(2,1)$ 和 $\mathrm{M}_p(1,1,1)$ 之一. 另外, 若 $k=n$ 或 $k=1$ 或 G 循环, 我们得不到任何有用的信息. 故以下假设所讨论的群 G 满足条件: $2\leqslant k\leqslant n-1$, $|G|=p^n,p>2,n\geqslant 4$ 且 G 非循环. 本节分类满足 $\mathrm{I}_k(G)\cong\mathrm{C}_{p^{k-1}}$ 的有限 p 群 G.

以下两个结果是简单的但经常被用到.

引理 14.9.1　设 $|G|=p^n$ 且 $|\mathrm{I}_k(G)|=p^{k-1}$. 则

(1) G 的秩 $r(G)>1$.

(2) 设 $H\leqslant G$. 若 $|H|\geqslant p^k$, 则 $\mathrm{I}_k(G)\leqslant\mathrm{I}_k(H)$.

(3) $\mathrm{I}_k(G)\leqslant\mathrm{I}_{k+1}(G)$; 特别地, $\mathrm{I}_k(G)\leqslant\Phi(G)$.

引理 14.9.2　设 G 为 p^n 阶群. 若 $\exp(G)=p^{n-1}$, 则 $\mathrm{I}_k(G)\cong\mathrm{C}_{p^{k-1}}$, 其中 $1\leqslant k\leqslant n-1$.

证明　令 $\mathrm{C}_{p^{n-1}}\cong M\leqslant G$, $H\leqslant G$ 满足 $|H|=p^k$. 则

$$|H\bigcap M|=\frac{|H||M|}{|HM|}\geqslant\frac{|H||M|}{|G|}=\frac{p^kp^{n-1}}{p^n}=p^{k-1}.$$

故 $H\bigcap M$ 含有 M 的唯一的 p^k 阶子群. 因为 G 不循环, 由 [89] 中的III, 定理 8.3 可知, $|\mathrm{I}_k(G)|\neq p^k$. 从而 $\mathrm{I}_k(G)\cong \mathrm{C}_{p^{k-1}}$. □

引理 14.9.3　若 $\mathrm{I}_2(G)\cong \mathrm{C}_p$, 则 $r(G)=2$.

证明　因为 G 不循环, 故 $r(G)>1$. 若 $r(G)\geqslant 3$, 则存在 $H\leqslant G$ 使得 $H\cong \mathrm{C}_p^3$. 于是 $\mathrm{I}_2(G)\leqslant \mathrm{I}_2(H)=\Phi(H)=1$, 矛盾. □

定理 14.9.4　*设 G 为 p^n 阶交换群, k 为满足 $2\leqslant k\leqslant n-2$ 的任意给定的正整数. 则 G 满足性质 $|\mathrm{I}_k(G)|=p^{k-1}$ 当且仅当 $G\cong \mathrm{C}_{p^{n-1}}\times \mathrm{C}_p$.*

证明　$\Longleftarrow$: 由引理 14.9.2 即得.

$\Longrightarrow$: 对 $|G|$ 进行归纳. 当 $n=4$ 时, 结论成立.

假设 $n\leqslant m$ 时, 结论成立. 下证 $n=m+1$ 时结论成立.

当 $n=m+1$ 时, 则 $k\leqslant m-1$. 取 G 的 p^{k+1} 阶非循环子群 H. 由引理 14.9.1(2) 知: $|\mathrm{I}_k(H)|\geqslant |\mathrm{I}_k(G)|=p^{k-1}$. 又 $|\mathrm{I}_k(H)|=|\Phi(H)|\leqslant p^{k-1}$. 故 $|\mathrm{I}_k(H)|=p^{k-1}$. 由归纳假设可知: $H\cong \mathrm{C}_{p^k}\times \mathrm{C}_p$. 因此 $\exp(G)\geqslant p^k$.

断言 $d(G)=2$. 若否, 则存在 G 的子群 $M\cong \mathrm{C}_{p^k}\times \mathrm{C}_p\times \mathrm{C}_p$, 则 $|\mathrm{I}_k(G)|\leqslant |\mathrm{I}_k(M)|\leqslant p^{k-2}$, 矛盾. 再证 $G\cong \mathrm{C}_{p^{n-1}}\times \mathrm{C}_p$. 若否, 存在 G 的子群 $N\cong \mathrm{C}_{p^k}\times \mathrm{C}_{p^2}$, 则 $|\mathrm{I}_k(G)|\leqslant |\mathrm{I}_k(N)|\leqslant p^{k-2}$, 矛盾. □

对于非交换的情况, 分 $k=2$ 和 $k>2$ 两种情况讨论.

引理 14.9.5　*设 G 是 p^n 阶的亚循环群. 则 $\mathrm{I}_2(G)\cong \mathrm{C}_p$ 当且仅当 $G\cong \mathrm{M}_p(n-1,1)$.*

证明　$\Longleftarrow$: 由引理 14.9.2 即得.

$\Longrightarrow$: 首先断言: $|\Omega_2(G)|\leqslant p^3$. 若否, 因为 G 亚循环且 $p>2$, 由 [89] 中的 Satz III. 10.2 可知, G 正则. 又由 [247] 中的引理 5.1.6(3) 可得, $\exp(\Omega_2(G))\leqslant p^2$. 因为 $\Omega_2(G)$ 循环, 故 $|\Omega_2(G)|\leqslant p^4$. 若 $|\Omega_2(G)|=p^4$, 由 p^4 阶群的分类可知, $\Omega_2(G)\cong \mathrm{C}_{p^2}\times \mathrm{C}_{p^2}$ 或 $\mathrm{M}_p(2,2)$. 由此可得 $\mathrm{I}_2(\Omega_2(G))=1$. 于是 $\mathrm{I}_2(G)=1$. 矛盾.

因为 G 非循环且正则, 由 [247] 中的定理 2.4.4 可得, $\omega(G)=2$. 于是 G 有唯一性基 a,b 使得 $G=\langle a\rangle\langle b\rangle$ 且 $\langle a\rangle\bigcap\langle b\rangle=1$. 设 $o(a)=p^m$, $o(b)=p^l$. 若 m, l 不同时为 1, 则 $\langle a^{p^{m-2}}\rangle\langle b^{p^{l-2}}\rangle\leqslant \Omega_2(G)$. 但是 $|\langle a^{p^{m-2}}\rangle\langle b^{p^{l-2}}\rangle|=p^4$. 这与 $|\Omega_2(G)|\leqslant p^3$ 矛盾. 不妨设 $l=1$. 则 $\langle a\rangle$ 是 G 的极大子群. 由 [26] 中的定理 1.2 即知 $G\cong \mathrm{M}_p(n-1,1)$. □

引理 14.9.6　*设 G 是极大类 3 群. 则 $\mathrm{I}_2(G)\cong \mathrm{C}_3$ 当且仅当 G 同构于下列互不同构的群之一.*

(1) $\langle a,b\mid a^9=b^3=c^3=1,[a,b]=c,[c,a]=1,[c,b]=a^{3v}\rangle$, *其中* $v=1$ *或* 2;

(2) $\langle a,b\mid a^9=c^3=1,b^3=a^3,[a,b]=c,[c,b]=a^{-3},[c,a]=1\rangle$.

证明　由 [26] 中的定理 1.2 可知, G 没有循环极大子群. 又由 [26] 中的定理 1.2 可知, G 的二步中心化子 K_2 是 G 的极大子群. 由此可得 K_2 不循环. 特

别地, K_2 至少有两个 9 阶子群. 于是 $|\mathrm{I}_2(K_2)| \leqslant 3$. 因为 $|\mathrm{I}_2(K_2)| \geqslant |\mathrm{I}_2(G)| = 3$, 故 $|\mathrm{I}_2(K_2)| = 3$. 若 $n \geqslant 5$, 由 [247] 中的定理 8.1.3 可得 K_2 是绝对正则的, 即, $|K_2 : \mho_1(K_2)| \leqslant 3^2$. 由 [247] 中的定理 2.4.4 可得 K_2 亚循环. 由定理 14.9.4 和引理 14.9.5 可得, $K_2 \cong \mathrm{C}_{3^{n-1}} \times \mathrm{C}_3$ 或 $\mathrm{M}_3(n-1,1)$. 所以 $\mho_{n-3}(K_2) \cong \mathrm{C}_9$. 因为 $\mho_{n-3}(K_2)$ char $K_2 \trianglelefteq G$, 故 $\mho_{n-3}(K_2) \trianglelefteq G$. 但是由 [247] 中的推论 8.1.4 可得, G 没有 9 阶循环正规子群, 矛盾. 故 $n = 4$. 由 [247] 中的定理 2.5.8 可知, G 是下列群之一:

(1′) $\langle a, b \mid a^9 = b^3 = c^3 = 1, [a,b] = c, [c,a] = a^3, [c,b] = 1\rangle$;

(2′) $\langle a, b \mid a^9 = c^3 = 1, b^3 = a^3, [a,b] = c, [c,b] = a^{-3}, [c,a] = 1\rangle$;

(3′) $\langle a, b \mid a^9 = b^3 = c^3 = 1, [a,b] = c, [c,a] = 1, [c,b] = a^{3v}\rangle$, 其中 $v = 1$ 或 2.

若 G 为群 (1′), 则存在 $H_1 = \langle a\rangle \cong \mathrm{C}_9$ 且 $H_2 = \langle b\rangle \times \langle c\rangle \cong \mathrm{C}_3 \times \mathrm{C}_3$ 使得 $H_1 \bigcap H_2 = 1$. 故 $\mathrm{I}_2(G) = 1$. 矛盾于假设.

若 G 为群 (2′), 则 $\Omega_1(G) = \langle a^3\rangle \times \langle c\rangle$. 设 $g \in G$ 且 $g^3 \neq 1$. 可证: $\langle g^3\rangle = \langle a^3\rangle$. 事实上, 不妨设 $g = a^i c^j b^k$. 由徐公式计算就有

$$
\begin{aligned}
g^3 &= (a^i c^j b^k)^3 = (a^i c^j)^3 [a^i c^j, b^{-k}]^3 [a^i c^j, b^{-k}, b^{-k}][a^i c^j, b^{-k}, a^i c^j] b^{3k} \\
&= a^{3i}[a^i, b^{-k}, b^{-k}][a^i, b^{-k}, a^i] b^{3k} = a^{3i} a^{3ik^2} a^{3k} = a^{3(i+ik^2+k)}.
\end{aligned}
$$

因为 $g^3 \neq 1$, 故 $(3, i+ik^2+k) = 1$. 于是 $\langle g^3\rangle = \langle a^3\rangle$. 这意味着 $\langle a^3\rangle$ 含在所有 3^2 阶循环子群里. 若 3^2 阶子群不循环, 则 $H \leqslant \Omega_1(G)$. 由此可得 $\mathrm{I}_2(G) = \langle a^3\rangle \cong \mathrm{C}_3$. 此为引理中的群 (2).

若 G 为群 (3′), 同上的方法, 类似可证 $\mathrm{I}_2(G) \cong \mathrm{C}_3$. 即引理中的群 (1). □

定理 14.9.7 设 G 是有限 p 群. 则 $\mathrm{I}_2(G) \cong \mathrm{C}_p$ 当且仅当 G 是下列互不同构的群之一.

(1) $\mathrm{C}_{p^{n-1}} \times \mathrm{C}_p$; (2) $\mathrm{M}_p(n-1,1)$; (3) $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^{n-2}}$;

(4) $\langle a, b \mid a^9 = c^3 = 1, b^3 = a^3, [a,b] = c, [c,b] = a^{-3}, [c,a] = 1\rangle$($p^4$ 阶群);

(5) $\langle a, b \mid a^{p^{n-2}} = 1, b^p = c^p = 1, [a,b] = c, [b,c] = a^{ip^{n-3}}, [c,a] = 1\rangle$, 其中 $i = 1$ 或 i 是模 p 的平方非剩余.

证明 由引理 14.9.3 可得 $r(G) = 2$. 特别地, G 的正规秩 $r_n(G) = 2$. 由 [31] 中的定理 4.1 可知, G 是下列互不同构的群之一:

(Ⅰ) 亚循环 p 群;

(Ⅱ) 极大类 3 群;

(Ⅲ) $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^{n-2}}$;

(Ⅳ) $\langle a, b \mid a^{p^{n-2}} = 1, b^p = c^p = 1, [a,b] = c, [b,c] = a^{ip^{n-3}}, [c,a] = 1\rangle$, 其中 $i = 1$ 或模 p 的平方非剩余.

若 G 亚循环, 由定理 14.9.4 和引理 14.9.5 可得, G 是定理中的群 (1) 和 (2).

若 G 是极大类 3 群, 由引理 14.9.6 可得, G 是定理中的群 (3) 和 (4), 其中 $p=3,\ n=4$.

若 G 是群 (III), 下证 $\mathrm{I}_2(G)\cong \mathrm{C}_p$. 显而易见, $\Omega_1(G)=\mathrm{M}_p(1,1,1)$. 于是

$$\mathrm{I}_2(\Omega_1(G))=\Phi(\Omega_1(G))=Z(\Omega_1(G))\cong \mathrm{C}_p.$$

注意到 $\Omega_2(G)=\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^2}$. 令

$$g\in\Omega_2(G),\quad o(g)=p^2,\quad g=a^ib^jd^k,\quad \text{其中 } i,\ j=0,\cdots,p-1,\quad (k,p)=1.$$

则 $g^p=(a^ib^jd^k)^p=(d^k)^p=d^{kp}$. 由此可得 $\langle g^p\rangle=\langle d^p\rangle=Z(\Omega_1(G))$. 这意味着 $\Omega_2(G)$ 的所有 p^2 循环子群包含 $Z(\Omega_1(G))$. 从而 $\mathrm{I}_2(G)\cong \mathrm{C}_p$.

若 G 是群 (IV), 下证 $\mathrm{I}_2(G)\cong \mathrm{C}_p$. 首先证明:

$$\Omega_2(G)=\langle b,c,a^{p^{n-4}}\rangle\cong \mathrm{M}_p(1,1,1)*\mathrm{C}_{p^2}.$$

明显地, $\langle b,c,a^{p^{n-4}}\rangle\leqslant\Omega_2(G)$. 只需证 $\Omega_2(G)\leqslant\langle b,c,a^{p^{n-4}}\rangle$. 令 $g=a^ib^jc^k\in\Omega_2(G)$. 由定理 4.1.4(4) 可知, G 是 p^2 交换的. 计算可得

$$1=g^{p^2}=(a^ib^jc^k)^{p^2}=a^{ip^2}b^{jp^2}c^{kp^2}=a^{ip^2}.$$

由此可得 $p^{n-4}|i$. 故 $g\in\langle b,c,a^{p^{n-4}}\rangle$. 现在与群 (III) 中讨论方法类似可得, $\mathrm{I}_2(G)\cong \mathrm{C}_p$. □

引理 14.9.8 设 G 是 p^n 阶群, $n\geqslant 5$, k 是满足 $2\leqslant k\leqslant n-1$ 的任意一个固定的正整数. 若 $\mathrm{I}_k(G)\cong \mathrm{C}_{p^{k-1}}$, 则 $\mathrm{I}_2(G)\cong \mathrm{C}_p$.

证明 若否, 则首先可证下列两个事实.

(1) 对于 G 的任意两个子群 H_1 和 U_1, 若 $|H_1|=|U_1|=p^2$ 且 $H_1\neq U_1$, 则 $H_1\bigcap U_1\cong \mathrm{C}_p$.

(2) $\exp(G)=p$.

对于 (1), 明显地, 存在满足 $|H_2|=|U_2|=p^k$ 的 G 的子群 H_2 和 U_2 使得 $H_1\leqslant H_2$ 且 $U_1\leqslant U_2$. 因为 $\mathrm{C}_{p^{k-1}}\cong \mathrm{I}_k(G)\lessdot H_2$, 故

$$|\mathrm{I}_k(G)\bigcap H_1|=\frac{|\mathrm{I}_k(G)||H_1|}{|\mathrm{I}_k(G)H_1|}\geqslant\frac{|\mathrm{I}_k(G)||H_1|}{|H_2|}=\frac{p^{k-1}p^2}{p^k}=p.$$

同样地, $|\mathrm{I}_k(G)\bigcap U_1|\geqslant p$. 因 $\mathrm{I}_k(G)$ 循环, 故 $1<|H_1\bigcap U_1|<p^2$. 所以 $H_1\bigcap U_1\cong \mathrm{C}_p$.

对于 (2), 若否, 则存在 $L\cong \mathrm{C}_{p^2}$. 由 (1) 的结论可得: 对于 $L\neq H\leqslant G$ 且 $|H|=p^2$, 有 $L\bigcap H\cong \mathrm{C}_p$. 因为 L 循环, 故 $\mathrm{I}_2(G)\cong \mathrm{C}_p$. 与假设矛盾.

设 $N \trianglelefteq G$ 且 $|N| = p^2$. 由 (2) 可设 $N = \langle a, b\rangle$. 又由 N/C 定理可知, $|G/C_G(N)| \leqslant p$. 因为 $|G| \geqslant p^5$, 故 $|C_G(N)| \geqslant p^4$. 取 $x \in C_G(N) \setminus N$, $y \in C_G(N) \setminus \langle x, N\rangle$. 令 $M_1 = \langle x, a\rangle$, $M_2 = \langle y, b\rangle$. 则 $|M_1| = |M_2| = p^2$ 且 $M_1 \bigcap M_2 = 1$. 这与 (1) 矛盾. □

定理 14.9.9 设 G 是 p^n 阶群, k 是满足 $3 \leqslant k \leqslant n-1$ 的任意一个固定的正整数. 则 $\mathrm{I}_k(G) \cong \mathrm{C}_{p^{k-1}}$ 当且仅当 G 同构于 $\mathrm{C}_{p^{n-1}} \times \mathrm{C}_p$ 或 $\mathrm{M}_p(n-1, 1)$.

证明 若 $n = 4$, 检查 p^4 阶群的群表即可得结论. 不妨设 $n \geqslant 5$. 由引理 14.9.8 可知, G 是定理 14.9.7 中群之一.

由引理 14.9.2 可知, 定理 14.9.7 中的群 (1) 和 (2) 满足假设条件.

若 G 为定理 14.9.7 中的群 (3), 且 $k = n-1$, 则 $|\mathrm{I}_k(G)| = |\Phi(G)| = p^{n-3}$. 若 $k \leqslant n-2$, 则存在

$$H_1 = \langle a^{p^{n-2-k}}\rangle \cong \mathrm{C}_{p^k}, \quad H_2 = \langle b, c\rangle * \langle a^{p^{n-4-k}}\rangle \cong \mathrm{M}_p(1,1,1) * \mathrm{C}_{p^{k-2}}$$

使得 $H_1 \bigcap H_2 \cong \mathrm{C}_{p^{k-2}}$. 明显地, $\mathrm{I}_k(G) \leqslant H_1 \bigcap H_2$ 的阶 $\leqslant p^{k-2}$. 因而定理 14.9.7 中的群 (3) 不满足假设条件.

若 G 为定理 14.9.7 中的群 (5), 则

$$\mathrm{I}_{n-1}(G) = \Phi(G) = \langle a^p\rangle \times \langle c\rangle \cong \mathrm{C}_{p^{n-3}} \times \mathrm{C}_p.$$

若 $k \leqslant n-2$, 则 G 有两个 p^k 阶子群

$$H_3 = \langle a^{p^{n-2-k}}\rangle \cong \mathrm{C}_{p^k}, \quad H_4 = \langle b, c\rangle * \langle a^{p^{n-4-k}}\rangle \cong \mathrm{M}_p(1,1,1) * \mathrm{C}_{p^{k-2}}$$

使得 $H_3 \bigcap H_4 = \langle a^{p^{n-4-k}}\rangle$. 明显地, $|\langle a^{p^{n-4-k}}\rangle| = p^{k-2}$. 于是定理 14.9.7 中的群 (5) 也不满足假设条件. □

14.9.2 $|\mathrm{I}_3(G)|=4$ 的 2 群

对于 2^4 阶群 G, $|\mathrm{I}_3(G)| = |\Phi(G)| = 4$ 当且仅当 G 二元生成. 故以下假设所讨论的群 G 满足 $|G| = 2^n$ 且 $n \geqslant 5$. 本节分类满足 $|\mathrm{I}_3(G)| = 4$ 的有限 2 群 G.

引理 14.9.10 设 G 是 2^n 阶非交换群, $n \geqslant 5$. 若 $\mathrm{I}_3(G) \cong \mathrm{C}_2 \times \mathrm{C}_2$, 则 $\exp(G) = 4$ 且 G 是 T_4 群.

证明 由 $\mathrm{I}_3(G) \cong \mathrm{C}_2 \times \mathrm{C}_2$ 可知 $\exp(G) \leqslant 4$. 若 $\exp(G) = 2$, 则 G 交换. 因而 $\exp(G) = 4$.

下证 $\Phi(G) = \mathrm{I}_3(G)$. 由引理 14.9.1(3) 知 $\mathrm{I}_3(G) \leqslant \Phi(G)$. 故只需证明 $\Phi(G) \leqslant \mathrm{I}_3(G)$. 设 g 为 G 的一个 4 阶元, 则存在 G 的一个 8 阶子群 H 使得 $g \in H$. 于是 $g^2 \in \mho_1(H) = \Phi(H)$. 由于 $\mathrm{I}_3(G)$ 是 H 的极大子群, $\Phi(H) \leqslant \mathrm{I}_3(G)$. 故 $g^2 \in \mathrm{I}_3(G)$. 由 g 的任意性可得 $\Phi(G) = \mho_1(G) \leqslant \mathrm{I}_3(G)$.

再证 $\mho_1(G)=\Phi(G)=\mathrm{I}_3(G)\leqslant Z(G)$. 若否, 则存在 $a\in G$ 使得 $a^2\notin Z(G)$. 从而存在 $b\in G$ 使得 $[a^2,b]\neq 1$. 即 $[a,b]^2[a,b,a]\neq 1$. 又因为 $\exp(G')\leqslant\exp(\Phi(G))=2$, 所以 $[a,b]^2=1$. 故 $[a,b,a]\neq 1$. 令 $H=\langle a,b\rangle$. 则 $c(H)\geqslant 3$. 又因为 $H'\leqslant\Phi(G)=\mathrm{I}_3(G)$, 所以 $H'=\Phi(G)=\mathrm{I}_3(G)$. 进而 $H'=\Phi(H)$, 于是 $|H|=2^4$. 从而 H 为极大类 2 群. 此时 $H'\cong\mathrm{C}_4$, 与 $H'\cong\mathrm{C}_2\times\mathrm{C}_2$ 矛盾.

最后证 G 为 $\mathcal{T}_4$ 群. 对任意 $x,y\in G$ 且 $[x,y]\neq 1$, 令 $M=\langle x,y\rangle$. 由 $M'\leqslant G'\leqslant\Phi(G)$ 知: $\exp(M')=2$. 于是 $[x,y]^2=1$. 由 $c(M)\leqslant c(G)=2$, 从而 $M'=\langle[x,y],M_3\rangle\cong\mathrm{C}_2$. 由定理 1.7.7 知, M 为内交换群. 因为 $\Phi(M)\leqslant\Phi(G)$, 所以 $|\Phi(M)|=2$ 或 4. 若 $|\Phi(M)|=2$, 则 $|M|=8$. 对任意 $a,b\in G$, 则 $a^2\in\mho_1(G)$. 又 $[a^2,b]=[a,b]^2=1$, 所以 $\mho_1(G)\leqslant Z(G)$, 于是 $\mathrm{I}_3(G)=\mho_1(G)\leqslant Z(G)$. 又 $\mathrm{I}_3(G)\lessdot M$, 故 $\mathrm{I}_3(G)\leqslant Z(M)$, 从而 M 交换, 与 M 内交换矛盾. 故 $|\Phi(M)|=4$, 于是 $|M|=16$, 即 M 为 16 阶内交换群. 由 M 的任意性, 得 G 为 $\mathcal{T}_4$ 群. □

引理 14.9.11 设 G 是 2^n 阶非交换群, $n\geqslant 5$. 若 $\mathrm{I}_3(G)\cong\mathrm{C}_2\times\mathrm{C}_2$, 则 $\mathrm{I}_3(G\times\mathrm{C}_2^m)\ncong\mathrm{C}_2\times\mathrm{C}_2$, 其中 $m\geqslant 1$.

证明 由引理 14.9.10 知, $\exp(G)=4$, 则存在 $g\in G$ 使得 $o(g)=4$. 从而存在 $H=\langle g\rangle\times\langle c\rangle\cong\mathrm{C}_4\times\mathrm{C}_2$, 其中 $c\in\mathrm{C}_2^m$. 因 $|\mathrm{I}_3(G)\bigcap H|=2$, 由引理 14.9.1(2) 得 $|\mathrm{I}_3(G\times\mathrm{C}_2^m)|\leqslant|\mathrm{I}_3(G)\bigcap H|=2$, 从而 $\mathrm{I}_3(G\times\mathrm{C}_2^m)\ncong\mathrm{C}_2\times\mathrm{C}_2$. □

引理 14.9.12 设 G 为 2^n 阶非交换群. 则 G 具有性质 $\mathrm{I}_3(G)\cong\mathrm{C}_2\times\mathrm{C}_2$ 当且仅当 G 是下列互不同构的群之一.

(Ⅰ) $\langle a,b,c\mid a^4=b^4=1,c^2=a^2,[a,c]=b^2,[b,c]=a^2,[a,b]=1\rangle$;

(Ⅱ) $\langle a,b,c\mid a^4=b^4=c^2=1,[c,a]=b^2a^2,[c,b]=a^2,[b,a]=1\rangle$;

(Ⅲ) $\langle a_1,a_2,b,d\mid a_1^4=a_2^4=1,b^2=a_1^2,d^2=a_2^2,[a_1,a_2]=1,[a_1,b]=a_2^2,[a_2,b]=a_1^2,[a_1,d]=a_1^2,[a_2,d]=a_1^2a_2^2,[b,d]=1\rangle$.

证明 由引理 14.9.10 知 G 为 $\mathcal{T}_4$ 群. 再由文献 [7] 知, G 为下列互不同构的 7 种群之一:

(1) $\mathrm{M}_3(1,2)\times\mathrm{C}_2^n$, 其中 n 为整数.

(2) $H\times\mathrm{C}_2^n$. 其中 $H=K\rtimes\langle a\rangle$ 是 $K=\langle b_1\rangle\times\langle b_2\rangle\times\cdots\times\langle b_k\rangle\times\langle c_1\rangle\times\langle c_2\rangle\times\cdots\times\langle c_k\rangle\cong\mathrm{C}_2^{2k}$ 被 $\langle a\rangle$ 的循环扩张, 满足 $a^4=1$, $b_i^a=b_ic_i^{-1}$, $c_i^a=c_i$ 对任意的 $1\leqslant i\leqslant k$ 都成立. n 为非负整数, k 为正整数.

(3) $H\times\mathrm{C}_2^n$. 其中 $H=K\rtimes\langle b\rangle$ 是 $K=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_l\rangle\cong\mathrm{C}_4^l$ 被 $\langle b\rangle$ 的循环扩张, 满足 $a_i^b=a_i^{-1}$ 对任意的 $1\leqslant i\leqslant l$ 成立. n 为非负整数, l 为正整数.

(4) $H\times\mathrm{C}_2^n$. 其中 $H=\langle a_1,a_2\mid a_1^4=a_2^4=1,b^2=a_1^2,[a_1,b]=a_2^2,[a_2,b]=a_1^2,[a_1,a_2]=1\rangle$, n 为非负整数.

(5) $H\times\mathrm{C}_2^n$. 其中 $H=\langle a_1,a_2,b\mid a_1^4=a_2^4=1,\ b^2=a_1^2,d^2=a_2^2,[a_1,a_2]=1,[a_1,b]=a_2^2,\ [a_2,b]=a_1^2,\ [a_1,d]=a_1^2,\ [a_2,d]=a_1^2a_2^2,\ [b,d]=1\rangle$, n 为非负整数.

(6) $H_1 \times \mathrm{C}_2^n$, $H_1 = \langle a, b \mid a^2 = b^4 = c^4 = 1, [a,b] = c^2, [a,c] = [b,c] = 1\rangle$, 其中 n 为非负整数.

(7) $H_2 \times \mathrm{C}_2^m$, $H_2 = \langle a, b \mid a^2 = b^4 = c^4 = 1, [a,b] = c^2, [a,c] = b^2c^2, [b,c] = 1\rangle$, 其中 m 为非负整数.

下面我们对上述 7 种群进行检验.

对群 (1), 因 $\exp(G) = 8$, 由引理 14.9.10 知, $\mathrm{I}_3(G) \ncong \mathrm{C}_2 \times \mathrm{C}_2$. 对群 (2), 存在子群 $H_1 = \langle c_1\rangle \times \langle b_1\rangle \times \langle b_2\rangle$, $H_2 = \langle c_1\rangle \times \langle a\rangle$, $|H_1| = |H_2| = 8$, 使得 $H_1 \bigcap H_2 = \langle c_1\rangle \cong \mathrm{C}_2$. 因 $\mathrm{I}_3(G) \leqslant H_1 \bigcap H_2$, 故 $\mathrm{I}_3(G) \ncong \mathrm{C}_2 \times \mathrm{C}_2$. 同理可证: 群 (3) 中有 $\mathrm{I}_3(G) \ncong \mathrm{C}_2 \times \mathrm{C}_2$. 群 (6) 中, 存在子群 $H_3 = \langle b^2\rangle \times \langle c\rangle$, $H_4 = \langle a\rangle \times \langle c\rangle$, $|H_3| = |H_4| = 8$ 使得 $H_3 \bigcap H_4 = \langle c\rangle \cong \mathrm{C}_4$. 因 $\mathrm{I}_3(G) \leqslant H_3 \bigcap H_4$，故 $\mathrm{I}_3(G) \ncong \mathrm{C}_2 \times \mathrm{C}_2$. 由上述讨论可知, 群 (1), (2), (3), (6) 都不是所求的群.

对于群 (4), 计算可知 $\Omega_1(H) = Z(H)$ 并且 $\Omega_1(H) \cong \mathrm{C}_2 \times \mathrm{C}_2$. 因为 H 是 $\mathcal{T}_4$ 群及 $\exp H = 4$, 所以 H 的任意 8 阶子群 N 满足 $N \cong \mathrm{C}_4 \times \mathrm{C}_2$. 于是 $\Omega_1(N) \cong \mathrm{C}_2 \times \mathrm{C}_2$. 进而 $\Omega_1(N) = \Omega_1(H)$. 故 $\mathrm{I}_3(H) \cong \mathrm{C}_2 \times \mathrm{C}_2$. 又由引理 14.9.11 知, $\mathrm{I}_3(H \times \mathrm{C}_2^m) \ncong \mathrm{C}_2 \times \mathrm{C}_2$. 从而 H 是我们所求的群, 即定理中的群 (Ⅰ). 同样的方法可证明群 (5) 和 (7) 有 $\mathrm{I}_3(H) \cong \mathrm{C}_2 \times \mathrm{C}_2$. 又由引理 14.9.11 知, $\mathrm{I}_3(H \times \mathrm{C}_2^m) \ncong \mathrm{C}_2 \times \mathrm{C}_2$. 从而 H 是我们所求的群, 即定理中的群 (Ⅱ) 和 (Ⅲ). □

引理 14.9.13 *设 G 为 2^n 阶群, $n \geqslant 5$. 若 $|\mathrm{I}_3(G)| \geqslant 4$ 且 $\mathrm{I}_3(G)$ 循环, 则 G 是亚循环群.*

证明 首先断言条件是子群遗传的. 对 G 的任意子群 H, 由引理 14.9.1(2) 知: $|\mathrm{I}_3(H)| \geqslant |\mathrm{I}_3(G)| \geqslant 4$. 再来证 $\mathrm{I}_3(H)$ 循环. 若 $|\mathrm{I}_3(H)| = 4$, 则 $\mathrm{I}_3(H)$ 循环. 若 $|\mathrm{I}_3(H)| = 8$, 则 H 有且仅有一个 8 阶子群. 故 H 循环. 从而 $\mathrm{I}_3(H)$ 循环.

设 G 是极小阶反例, 则 G 是内亚循环群. 若 $n = 5$, 由定理 8.1.1 得

$$G = \langle a, b, c \mid a^4 = b^4 = 1, c^2 = a^2b^2, [a,c] = a^2, [b,c] = c^2, [a,b] = 1\rangle.$$

再由引理 14.9.12 知: $\mathrm{I}_3(G) \cong \mathrm{C}_2 \times \mathrm{C}_2$, 矛盾. 若 $n \geqslant 6$, 由定理 8.1.1 知: 没有阶大于等于 2^6 的内亚循环群, 矛盾. □

引理 14.9.14 *设 G 为 2^n 阶亚循环群, $n \geqslant 5$. 若 $\mathrm{I}_3(G) \cong \mathrm{C}_4$, 则 G 有循环极大子群.*

证明 用反证法, 假设 G 无循环极大子群. 由 [247] 中的引理 2.2.11 可知, G 中存在 $(2,2)$ 型的正规子群 M. 因为 $\mathrm{I}_3(G) \cong \mathrm{C}_4$, 所以 G 中包含 M 的 8 阶子群是唯一的. 从而 G/M 的 2 阶子群也唯一. 故 G/M 为循环群或者广义四元数群. 若 G/M 为循环群, 则 G 中存在二极大子群 $\langle a\rangle$ 循环, 且 $G = M \rtimes \langle a\rangle$, 这与 G 亚循环矛盾; 若 G/M 为广义四元数群, 则 G/M 中存在与 Q_8 同构的子群 H/M. 再设 N 是含于 M 的 G 的 p 阶正规子群, 则 H/N 为 16 阶群, 并且 H/N 有一个商

群同构于 Q_8. 由 16 阶群的分类可知, $H/N \cong M_2(2,2)$. 显然, $I_2(H/N) = 1$, 从而 $I_3(H) \leqslant N$. 由引理 14.9.1(2), 有 $I_3(G) \leqslant I_3(H) \leqslant N$, 仍与题设矛盾. □

定理 14.9.15　设 G 为 2^n 阶群, $n \geqslant 5$. 则 G 具有性质 $|I_3(G)| = 4$ 当且仅当 G 是下列互不同构的群之一:

(1) $C_{2^{n-1}} \times C_2$;　(2) $M_2(n-1,1)$;

(3) D_{2^n};　(4) Q_{2^n};　(5) SD_{2^n};

(6) $\langle a,b,c \mid a^4 = b^4 = 1, c^2 = a^2, [a,c] = b^2, [b,c] = a^2, [a,b] = 1\rangle$;

(7) $\langle a,b,c \mid a^4 = b^4 = c^2 = 1, [c,a] = b^2a^2, [c,b] = a^2, [b,a] = 1\rangle$;

(8) $\langle a_1,a_2,b,d \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, d^2 = a_2^2, [a_1,a_2] = 1, [a_1,b] = a_2^2, [a_2,b] = a_1^2, [a_1,d] = a_1^2, [a_2,d] = a_1^2a_2^2, [b,d] = 1\rangle$.

证明　若 G 是交换群, 由定理 14.9.4 知: G 是定理中的群 (1). 若 G 是非交换群且 $I_3(G) \cong C_4$, 由引理 14.9.13 知: G 是亚循环群. 再由引理 14.9.14 知, G 有循环极大子群. 再由定理 1.9.1 得, G 为定理中的群 (2)—(5). 若 G 是非交换群且 $I_3(G) \cong C_2 \times C_2$, 由引理 14.9.12 知: G 为定理中的群 (6)—(8).

反之, 由定理 14.9.4 知: 群 (1) 满足定理条件. 由引理 14.9.2 知, 群 (2)—(5) 满足定理条件. 由引理 14.9.12 知: 群 (6)—(8) 也满足定理条件.

同构问题是比较显然的. 群 (1) 是交换群, 其余都是非交换群. 群 (2)—(5) 是有循环极大子群的四类互不同构的群, 而群 (6)—(8) 是无循环极大子群的群. 又由文献 [31] 知, 群 (6)—(8) 是互不同构的.

14.9.3　$|I_{\mathcal{A}_1}(G)| \leqslant p^{n-3}$ 的 p^n 阶群

由于每个非交换群必含有一个内交换子群, 故群 G 的所有非交换子群的交恰是 G 的所有内交换子群的交. 本节分类 $|I_{\mathcal{A}_1}(G)|$ 分别为 p^{n-2} 和 p^{n-3} 的 p^n 阶群, 首先证明 $|I_{\mathcal{A}_1}(G)|$ 的几个性质.

引理 14.9.16　设 G 是非交换且非内交换的 p^n 阶群. 则

(1) $I_{\mathcal{A}_1}(G)$ 交换.

(2) $|I_{\mathcal{A}_1}(G)| \leqslant p^{n-2}$.

(3) 若 $|I_{\mathcal{A}_1}(G)| = p^{n-k}$, 其中 $2 \leqslant k \leqslant n-2$, 则 G 的所有 p^{n-k} 子群交换.

(4) 若 $|I_{\mathcal{A}_1}(G)| = p^{n-k}$, 其中 $2 \leqslant k$, 则 $d(G) \leqslant k$.

证明　(1) 和(2)显然成立.

(3) 若否, 设 k 是满足 $2 \leqslant k \leqslant n-3$ 的任意一个固定的正整数. 令 H 是 p^{n-k} 非交换子群. 则 $H \geqslant I_{\mathcal{A}_1}(G)$. 于是 $H = I_{\mathcal{A}_1}(G)$. 这与 (1) 矛盾.

(4) 若否, 设 $d(G) = d$. 则 G 的极大子群的个数为

$$1 + p + p^2 + \cdots + p^{d-1}.$$

令

$$t = 2 + p + p^2 + \cdots + p^{d-2}.$$

因为非交换 p 群的交换极大子群的个数至多是 $1+p$, 故 G 至少有 t 个非交换极大子群. 令 $M_1, M_2, M_3, \cdots, M_t$ 是 G 的 t 个非交换极大子群且 $N = \bigcap\limits_{i=1}^{t} M_i$. 因为 $M_i \lhd G$, 故 $N \lhd G$. 若 $|N| \geqslant p^{n-k}$, 则 G/N 的极大子群的个数至多是

$$1 + p + \cdots + p^{k-1}.$$

另一方面, 对每个 $i \in \{1, 2, \cdots, t\}$, M_i/N 是 G/N 的极大子群. 因为 $d > k$, 故

$$t > 1 + p + \cdots + p^{k-1}.$$

矛盾. 由此可得 $|N| < p^{n-k}$. 又因为 $\mathrm{I}_{\mathcal{A}_1}(G) \leqslant N$, 故

$$p^{n-k} = |\mathrm{I}_{\mathcal{A}_1}(G)| \leqslant |N| < p^{n-k}.$$

这又是一个矛盾. 故 $d(G) < k$. □

注 14.9.17 由引理 14.9.16(2)及 $\mathcal{A}_t$ 群的定义易得, 若 $|\mathrm{I}_{\mathcal{A}_1}(G)| = p^{n-k}$, 则对某个 t, $G \in \mathcal{A}_t$, 其中 $2 \leqslant t \leqslant k \leqslant n-2$. 特别地, 若 $|\mathrm{I}_{\mathcal{A}_1}(G)| = p^{n-2}$, 则 $G \in \mathcal{A}_2$.

定理 14.9.18 设 G 是非交换且非内交换的 p^n 阶群. 则 $|\mathrm{I}_{\mathcal{A}_1}(G)| = p^{n-2}$ 当且仅当 G 是二元生成的 $\mathcal{A}_2$ 群.

证明 $\Longrightarrow$: 由注 14.9.17 可得 $G \in \mathcal{A}_2$. 又有引理 14.9.16(4) 可得 $d(G) = 2$.

$\Longleftarrow$: 因为 $G \in \mathcal{A}_2$, 故 $\mathrm{I}_{\mathcal{A}_1}(G) \geqslant \Phi(G)$. 又 $d(G) = 2$, 故 $|\Phi(G)| = p^{n-2}$. 于是 $|\mathrm{I}_{\mathcal{A}_1}(G)| \geqslant p^{n-2}$. 由引理 14.9.16(2) 即得. □

下面分类满足 $|\mathrm{I}_{\mathcal{A}_1}(G)| = p^{n-3}$ 的 p^n 阶群.

引理 14.9.19 设 G 是 p^n 阶的 $\mathcal{A}_2$ 群. 则 $|\mathrm{I}_{\mathcal{A}_1}(G)| = p^{n-3}$ 当且仅当 $d(G) = 3$.

证明 $\Longrightarrow$: 若否, 由引理 14.9.16(4) 可得 $d(G) = 2$. 这矛盾于定理 14.9.18.

$\Longleftarrow$: 因为 $G \in \mathcal{A}_2$, 故 $\mathrm{I}_{\mathcal{A}_1}(G) \geqslant \Phi(G)$. 又 $d(G) = 3$, 故 $|\Phi(G)| = p^{n-3}$. 于是 $|\mathrm{I}_{\mathcal{A}_1}(G)| \geqslant p^{n-3}$. 另一方面, 由引理 14.9.16(2) 可得, $|\mathrm{I}_{\mathcal{A}_1}(G)| \leqslant p^{n-2}$. 再由 $d(G) = 3$ 及定理 14.9.18 可得, $|\mathrm{I}_{\mathcal{A}_1}(G)| \neq p^{n-2}$. 结论得证. □

引理 14.9.20 设 G 是非交换且非内交换的 p^n 阶群. 若 $|\mathrm{I}_{\mathcal{A}_1}(G)| = p^{n-3}$, 则 G 的所有非交换真子群是二元生成的.

证明 因为 $|\mathrm{I}_{\mathcal{A}_1}(G)| = p^{n-3}$, 故由注 14.9.17 可知, $G \in \mathcal{A}_2$ 或 $\mathcal{A}_3$. 若 $G \in \mathcal{A}_2$, 则 G 的所有非交换真子群是 $\mathcal{A}_1$ 群. 结论由定理 1.7.7 推出. 设 $G \in \mathcal{A}_3$. 注意到 $\mathcal{A}_3$ 群的每个真子群是 $\mathcal{A}_1$ 群或 $\mathcal{A}_2$ 群. 只需证 G 的每个 $\mathcal{A}_2$ 子群是二元生成的. 若否, 因为 $\mathcal{A}_2$ 的生成元个数至多是 3, 故存在 $M \in \mathcal{A}_2$ 使得 $d(M) = 3$. 由引理 14.9.19 可得, $|\mathrm{I}_{\mathcal{A}_1}(M)| = p^{(n-1)-3} = p^{n-4}$. 明显地, $\mathrm{I}_{\mathcal{A}_1}(M) \geqslant \mathrm{I}_{\mathcal{A}_1}(G)$. 从而 $|\mathrm{I}_{\mathcal{A}_1}(M)| \geqslant |\mathrm{I}_{\mathcal{A}_1}(G)|$. 矛盾. □

引理 14.9.21　设 G 是奇阶非亚循环的 $\mathcal{A}_3$ 群. 若 G 的每个 $\mathcal{A}_2$ 子群 H 是二元生成的, 则 $\Phi(H)=\mho_1(G)\Phi(G')G_3$.

证明　因为 G 是 $\mathcal{A}_3$ 群, 所以 G 的所有非交换真子群是 $\mathcal{A}_1$ 群或 $\mathcal{A}_2$ 群. 于是 G 的所有非交换真子群是二元生成的. 因而 $G\in\mathcal{B}_p'$ 且 $d(G)=2$ 或 $d(G)=3$.

首先断言: $d(G)\neq 3$. 若否, 则 $d(G)=3$. 若 G 有交换极大子群, 则 $G\in\mathcal{D}_p(3)$. 由 [246] 中的定理 4.1 推出 $G\in\mathcal{A}_2$. 与假设矛盾. 若 G 无交换极大子群, 由 $d(G)=3$ 可知, G 既非亚循环也非极大类 3 群. 于是 $G\in\mathcal{M'}_p$. 又由 $G\in\mathcal{A}_3$ 可得 $|G|\geqslant p^5$. 进一步地, 由 [246] 中的引理 5.3 可知, $|G|\neq p^5$. 由此可得 $|G|\geqslant p^6$. 因为 $G\in\mathcal{A}_3$ 以及 G 无交换极大子群, 由定理 1.7.7 及假设可得, G 的所有极大子群是二元生成的. 另一方面, p 是奇素数, 由 [31] 中的定理 3.1 可得, $|G|\leqslant p^5$. 矛盾. 于是 $d(G)=2$.

令 $\overline{G}=G/\Phi(G')G_3$. 因为 G 是二元生成的非亚循环群, 由 [247] 中的推论 2.4.2, 设

$$\overline{G}=\langle \bar{a},\bar{b},\bar{c}\mid \bar{a}^{p^{n_1}}=\bar{b}^{p^{m_1}}=\bar{c}^p=1,[\bar{a},\bar{b}]=\bar{c},[\bar{a},\bar{c}]=[\bar{b},\bar{c}]=1\rangle.$$

则

$$G/\mho_1(G)\Phi(G')G_3\cong\overline{G}/\overline{\mho_1(G)}=\overline{G}/\mho_1(\overline{G}).$$

因为 $p>2$, 故 $\mho_1(\overline{G})=\langle\bar{a}^p,\bar{b}^p\rangle$. 由此可得 $|\mho_1(\overline{G})|=p^{n_1+m_1-2}$. 进一步地,

$$|G/\mho_1(G)\Phi(G')G_3|=p^3.$$

于是

$$G/\mho_1(G)\Phi(G')G_3\cong\overline{G}/\overline{\mho_1(G)}$$

是 p^3 阶的 $\mathcal{A}_1$ 群且 $\exp(G)=p$. 因而 $H/\mho_1(G)\Phi(G')G_3$ 是 p^2 阶的初等交换群. 现在有

$$\Phi(H)\mho_1(G)\Phi(G')G_3/\mho_1(G)\Phi(G')G_3\leqslant\Phi(H/\mho_1(G)\Phi(G')G_3)=1.$$

因而 $\Phi(H)\leqslant\mho_1(G)\Phi(G')G_3$. 因为 $H\lessdot G$ 且 $d(H)=2$, 故 $|\Phi(H)|=p^{n-3}$. 另一方面, $|G/\mho_1(G)\Phi(G')G_3|=p^3$. 由此可得 $\Phi(H)=\mho_1(G)\Phi(G')G_3$. □

定理 14.9.22　设 G 是非交换且非内交换的 p^n 阶群. 则

(1) 若 G 非亚循环, 则 $|\mathrm{I}_{\mathcal{A}_1}(G)|=p^{n-3}$ 当且仅当 G 是三元生成的 $\mathcal{A}_2$ 群或是非交换真子群均二元生成的 $\mathcal{A}_3$ 群.

(2) 若 G 亚循环, 则 $|\mathrm{I}_{\mathcal{A}_1}(G)|=p^{n-3}$ 当且仅当 $p=2$ 且 G 是下列群之一:

(2.1) D_{32}, 二面体群;

(2.2) Q_{32}, 广义四元数群;

(2.3) SD_{32}, 半二面体群;

(2.4) 有交换极大子群的例外亚循环 $\mathcal{A}_3$ 群.

证明 (1) $\Longrightarrow$: 由引理 14.9.20 可得, G 的非交换真子群均二元生成. 又由引理 14.9.16(3) 可得, G 的所有 p^{n-3} 阶子群均交换. 于是由注 14.9.17 可得, $G \in \mathcal{A}_2$ 或 $\mathcal{A}_3$. 若 $G \in \mathcal{A}_2$, 则由引理 14.9.19 即得.

$\Longleftarrow$: 若 G 是三元生成的 $\mathcal{A}_2$ 群, 则由引理 14.9.19 可得 $|\mathrm{I}_{\mathcal{A}_1}(G)| = p^{n-3}$.

设 G 是 $\mathcal{A}_3$ 群. 首先断言: G 不是 2 群. 若否, 则 $G \in \mathcal{D}_2$ 或 $\mathcal{M}_2$. 若 $G \in \mathcal{D}_2$, 则 $d(G) = 2$ 或 3. 因而 $G \in \mathcal{D}_2(2)$ 或 $\mathcal{D}_2(3)$. 若 $G \in \mathcal{D}_2(3)$, 则由 [246] 中的定理 4.1 可得 $G \in \mathcal{A}_2$, 矛盾. 若 $G \in \mathcal{D}_2(2)$, 则由 [246] 中的推论 3.8 可得 G 亚循环, 矛盾. 若 $G \in \mathcal{M}_2$, 因为 G 既非亚循环也非极大类 3 群, 故 $G \in \mathcal{M}_2'$. 由 [246] 中的定理 5.2 可得 $G \in \mathcal{A}_2$, 也是一个矛盾.

现在由引理 14.9.16(2) 可得 $|\mathrm{I}_{\mathcal{A}_1}(G)| \leqslant p^{n-2}$. 另一方面, 由定理 14.9.18 可得 $|\mathrm{I}_{\mathcal{A}_1}(G)| \leqslant p^{n-3}$. 令 S 是 G 的所有 $\mathcal{A}_2$ 子群的集合. 则

$$\mathrm{I}_{\mathcal{A}_1}(G) \geqslant \Phi(G) \bigcap \left(\bigcap_{M \in S} \Phi(M) \right).$$

再令 H 是 G 的一个 $\mathcal{A}_2$ 子群. 因为 G 不是 2 群, 由引理 14.9.21 可得

$$\bigcap_{M \in S} \Phi(M) = \Phi(H) = \mho_1(G)\Phi(G')G_3.$$

又 $d(H) = 2$, 故 $|\Phi(H)| = p^{(n-1)-2} = p^{n-3}$. 于是

$$|\mathrm{I}_{\mathcal{A}_1}(G)| \geqslant |\Phi(G) \bigcap \Phi(H)| = |\Phi(H)| = p^{n-3}.$$

由此可得 $|\mathrm{I}_{\mathcal{A}_1}(G)| = p^{n-3}$.

(2) $\Longrightarrow$: 由注 14.9.17 可知, $G \in \mathcal{A}_2$ 或 $\mathcal{A}_3$. 又由 [27] 中的命题 72.1 可得, $|G'| = p^2$ 或 $|G'| = p^3$. 若 $G \in \mathcal{A}_2$, 由引理 14.9.19 可得 $d(G) = 3$. 然而, 不存在这样的亚循环群. 故 G 是亚循环的 $\mathcal{A}_3$ 群. 通过检查亚循环群的分类, 即定理 6.1.3 和定理 6.1.4 可得 G 是下列群之一.

(i) 奇数阶亚循环的 $\mathcal{A}_3$ 群

$$\langle a, b \mid a^{p^{r+3}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r} \rangle,$$

其中 r, s, t 是非负整数且 $r \geqslant 1$.

(ii) 通常亚循环 $\mathcal{A}_3$ 群, 即

$$\langle a, b \mid a^{2^{r+3}} = 1, b^{2^{r+s+t}} = a^{2^{r+s}}, a^b = a^{1+2^r} \rangle,$$

其中 r, s, t 是非负整数且 $r \geqslant 2$.

(iii) 例外亚循环 $\mathcal{A}_3$ 群, 即 $\langle a,b \mid a^{2^{r+s+v+t'+u}}=1, b^{2^{r+s+t}}=a^{2^{r+s+v+t'}}, a^b=a^{-1+2^{r+v}}\rangle$, 其中 r,s,t,t' 和 v 是非负整数, $r+s+v+t'+u=4$, $r\geqslant 2$, $t'\leqslant r, u\leqslant 1$, $tt'=sv=tv=0$.

(iv) 有循环极大子群的亚循环 $\mathcal{A}_3$ 群, 即 D_{32}, Q_{32} 和 SD_{32}.

若 G 是群(i), 则 $\langle a^{p^2},b\rangle$ 和 $\langle a,b^{p^2}\rangle$ 非交换. 进一步地,

$$|\langle a^{p^2},b\rangle\bigcap\langle a,b^{p^2}\rangle|=|\langle a^{p^2},b^{p^2}\rangle|=p^{2r+s+t-1}.$$

故 $|\mathrm{I}_{A_1}(G)|\leqslant p^{n-4}$. 于是群(i)不是满足条件的群.

若 G 是群(ii), 我们观察到 $|\langle a^4,b\rangle\bigcap\langle a,b^4\rangle|=|\langle a^4,b^4\rangle|$. 故 $|\mathrm{I}_{\mathcal{A}_1}(G)|\leqslant 2^{n-4}$. 于是群(ii)也不是满足条件的群.

若 G 是群(iii), 考虑 G 的所有非交换子群.

首先, G 的所有极大子群分别是

$$M_1=\langle a,b^2\rangle,\quad M_2=\langle a^2,b\rangle,\quad M_3=\langle ba,a^2\rangle.$$

又 M_1 的所有极大子群分别是

$$M_{11}=\langle a,b^4\rangle,\quad M_{12}=\langle b^2,a^2\rangle,\quad M_{13}=\langle b^2a,a^2\rangle.$$

M_2 的所有极大子群分别是

$$M_{21}=\langle a^2,b^2\rangle,\quad M_{22}=\langle b,a^4\rangle,\quad M_{23}=\langle ba^2,a^4\rangle.$$

M_3 的所有极大子群分别是

$$M_{31}=\langle a^2,b^2\rangle,\quad M_{32}=\langle ba,a^4\rangle,\quad M_{33}=\langle ba^3,a^4\rangle.$$

因为 $r+s+v+t'+u=4$ 且 $r\geqslant 2$, 故 $s+t'+u=0,1$ 或 2. 若 $s+t'+u=0$ 或 1, 则 $Z(G)=\langle a^{2^3}\rangle\langle b^2\rangle$. 若 $s+t'+u=2$, 则 $Z(G)=\langle a^{2^3}\rangle\langle b^4\rangle$.

若 G 无交换极大子群, 则 $b^2\notin Z(G)$. 由引理 14.9.16(3) 可知, G 的所有 p^{n-3} 的子群是交换的, 故 G 的所有非交换子群可从上面所列的子群中挑出, 即

$$M_1,\ M_2,\ M_3,\ M_{11},\ M_{12},\ M_{13},\ M_{21},\ M_{22},\ M_{23}, M_{31},\ M_{32},\ M_{33}.$$

易验证, 所有这些子群的交 $\mathrm{I}_{\mathcal{A}_1}(G)=\langle a^4,b^4\rangle$. 故 $|\mathrm{I}_{\mathcal{A}_1}(G)|=p^{n-4}$. 这与假设矛盾. 因而 G 有交换极大子群.

若 G 有交换极大子群, 则 $b^2\in Z(G)$. 此时 G 的所有非交换极大子群分别是

$$M_2,\ M_3,\ M_{22},\ M_{23},\ M_{32},\ M_{33}.$$

易验证, 所有这些子群的交 $\mathrm{I}_{\mathcal{A}_1}(G)=\langle a^4,b^2\rangle$. 故 $|I_{\mathcal{A}_1}(G)|=p^{n-3}$.

若 G 是群 $\mathrm{D}_{32},\mathrm{Q}_{32}$ 或 SD_{32} 之一, 通过简单的计算可知 $|\mathrm{I}_{\mathcal{A}_1}(G)|=p^{n-3}$.

$\Longleftarrow$: 上述证明过程已给出要证的结论. □

注 14.9.23 三元生成的 $\mathcal{A}_2$ 群在 [280] 中的引理 2.5 被列出. 文献 [280] 分类了 $\mathcal{A}_3$ 群, 文献[246]分类了非交换真子群均二元生成的有限 p 群. 通过对 [246] 中的主要定理和 [280] 的一个简单的检查可得, 非交换真子群均二元生成的非亚循环 $\mathcal{A}_3$ 群是文献 [280] 中的定理 5.1 列出的群 (F4)—(F8) 以及文献 [280] 中的定理 5.1 列出的群 (K3)—(K5). 有交换极大子群的例外亚循环的 $\mathcal{A}_3$ 群是文献 [280] 中的定理 5.1 列出的群 (F1)—(F3). 所以满足 $|\mathrm{I}_{\mathcal{A}_1}(G)|=p^{n-3}$ 的 p^n 阶群是被分类.

14.9.4 $\Phi_{N\mathcal{A}_1M}(G)>\Phi(G)$ 的 p 群

本节所述内容的源动力来自 Berkovich 在其专著 [28] 提出的下列问题.

Problem 1576(i) Let $H\not\leqslant\Phi(G)$ be a normal subgroup of a p group G. Study the structure of G provided all maximal subgroups of G not containing H are minimal nonabelian.

为方便, Problem 1576(i) 中的群称为 $\mathcal{B}$ 群. 本节分类 $\mathcal{B}$ 群. 首先对 $\mathcal{B}$ 群作如下分析. 若 G 是 $\mathcal{B}$ 群, 则 G 至少有一个极大子群不含 H, 因而 G 至少有一个极大子群是内交换的. 另一方面, 我们知道, 若 p 群 G 的所有极大子群是交换或内交换, 则 G 是 $\mathcal{A}_2$ 群. 而 $\mathcal{A}_2$ 群已被分类, 因而可设 $\mathcal{B}$ 群至少含有一个极大子群既非交换也非内交换. 而恰有一个极大子群既非交换也非内交换的有限 p 群被 Janko 等在系列论文 [38],[100],[101] 分类. 故不失一般性可设 $\mathcal{B}$ 群至少含有两个极大子群既非交换也非内交换. 称这样的群为 $\mathcal{B}^*$ 群. 故分类 $\mathcal{B}$ 群可归结为分类 $\mathcal{B}^*$ 群.

张丽华在文献 [267] 引进了一个新的子群概念: 有限 p 群 G 的所有非内交换的极大子群的交, 记为 $\Phi_{N\mathcal{A}_1M}(G)$, 即

$$\Phi_{N\mathcal{A}_1M}(G)=\bigcap_{\substack{M\lessdot G\\ M\notin\mathcal{A}_1}}M.$$

其中 $M\lessdot G$ 表示 M 是 G 的极大子群, $M\notin\mathcal{A}_1$ 表示 M 不是 G 的 $\mathcal{A}_1$ 子群. 明显地, $\Phi_{N\mathcal{A}_1M}(G)$ 是 G 的特征子群. 下面讨论 $\Phi_{N\mathcal{A}_1M}(G)$ 与 $\mathcal{B}$ 群和 $\mathcal{B}^*$ 群的关系.

定理 14.9.24 有限 p 群 G 是 $\mathcal{B}$ 群当且仅当 $\Phi_{N\mathcal{A}_1M}(G)>\Phi(G)$.

证明 $\Longrightarrow$: 明显地, $\Phi_{N\mathcal{A}_1M}(G)\geqslant\Phi(G)$. 令 $H\not\leqslant\Phi(G)$ 且 $H\trianglelefteq G$. 因为 G 是 $\mathcal{B}$ 群, 故 G 的不含 H 的极大子群均内交换. 因而 G 的非内交换的极大子群均包含 H. 由此可得 $H\leqslant\Phi_{N\mathcal{A}_1M}(G)$. 因为 $H\not\leqslant\Phi(G)$, 故 $\Phi_{N\mathcal{A}_1M}(G)>\Phi(G)$.

$\Longleftarrow$: 令 $H=\Phi_{N\mathcal{A}_1M}(G)$. 则 $H\trianglelefteq G$. 因为 $\Phi_{N\mathcal{A}_1M}(G)>\Phi(G)$, 故 $H\not\leqslant\Phi(G)$. 明显地, G 的不含 H 的极大子群均内交换. 因而 G 是 $\mathcal{B}$ 群. □

命题 14.9.25 设 G 是有内交换极大子群的有限 p 群. 则 $|G:\Phi_{N\mathcal{A}_1M}(G)|\leqslant p^3$.

证明 令 M 是 G 的一个内交换极大子群. 由定理 1.7.7 可知 $d(M)=2$. 因而 $d(G)\leqslant 3$. 因为 $\Phi(G)\leqslant\Phi_{N\mathcal{A}_1M}(G)$, 故

$$|G:\Phi_{N\mathcal{A}_1M}(G)|\leqslant|G:\Phi(G)|=p^{d(G)}\leqslant p^3.$$ □

命题 14.9.26 设 G 是有限 p 群. 若 G 至少有一个极大子群是内交换的, 也至少有一个极大子群不是内交换的, 则下列陈述等价.

(1) $|G:\Phi_{N\mathcal{A}_1M}(G)|=p$.

(2) 除 $\Phi_{N\mathcal{A}_1M}(G)$ 之外, G 的所有极大子群是内交换的.

证明 (2)$\Longrightarrow$(1) : 显然.

(2)$\Longleftarrow$(1): 因为 $|G:\Phi_{N\mathcal{A}_1M}(G)|=p$, 故 $\Phi_{N\mathcal{A}_1M}(G)$ 是 G 的极大子群. 令 M 是 G 的非内交换的极大子群. 则 $\Phi_{N\mathcal{A}_1M}(G)\leqslant M$. 因而 $\Phi_{N\mathcal{A}_1M}(G)=M$, 即 $\Phi_{N\mathcal{A}_1M}(G)$ 是 G 的唯一的非内交换的极大子群. □

注 14.9.27 若 G 是 $\mathcal{B}^*$ 群, 则 $|G:\Phi_{N\mathcal{A}_1M}(G)|\neq p$.

命题 14.9.28 设 G 是有限 p 群. 若 G 至少有一个极大子群是内交换的, 也至少有两个极大子群不是内交换的, 则下列陈述等价.

(1) $|G:\Phi_{N\mathcal{A}_1M}(G)|=p^2$;

(2) G 的任意两个不同的非内交换极大子群的交等于 $\Phi_{N\mathcal{A}_1M}(G)$.

证明 (1) $\Longrightarrow$ (2): 设 M_1 和 M_2 是两个非内交换的极大子群. 则 $\Phi_{N\mathcal{A}_1M}(G)\leqslant M_1\bigcap M_2$. 因为 $|G:\Phi_{N\mathcal{A}_1M}(G)|=p^2$, 故 $M_1\bigcap M_2=\Phi_{N\mathcal{A}_1M}(G)$.

(1) $\Longleftarrow$ (2): 设 M_1 和 M_2 是两个非内交换的极大子群. 由假设得, $M_1\bigcap M_2=\Phi_{N\mathcal{A}_1M}(G)$. 注意到 $M_1\bigcap M_2$ 是 G 的 2 极大子群. 因而 $|G:\Phi_{N\mathcal{A}_1M}(G)|=|G:M_1\bigcap M_2|=p^2$. □

下列两个命题是简单的, 但经常用到. 我们将其列出, 读者自证.

命题 14.9.29 设 G 是有限 p 群且满足条件: G 至少有一个极大子群是内交换的, 也至少有一个极大子群不是内交换的. 若 $|G:\Phi_{N\mathcal{A}_1M}(G)|=p^2$, 则

(1) 若 $d(G)=2$, 则 $\Phi_{N\mathcal{A}_1M}(G)=\Phi(G)$.

(2) 若 $d(G)=3$, 则 $\Phi_{N\mathcal{A}_1M}(G)>\Phi(G)$.

命题 14.9.30 设 G 是有限 p 群且满足条件: G 至少有一个极大子群是内交换的, 也至少有一个极大子群不是内交换的. 若 $|G:\Phi_{N\mathcal{A}_1M}(G)|=p^3$, 则 $\Phi_{N\mathcal{A}_1M}(G)=\Phi(G)$.

命题 14.9.25、命题 14.9.29、命题 14.9.30、注 14.9.27 以及定理 14.9.24 的直接结果是如下结论.

推论 14.9.31 设 G 是 $\mathcal{B}^*$ 群. 则

(1) $|G:\Phi_{N\mathcal{A}_1M}(G)|=p^2$ 且 $d(G)=3$.

(2) G 至多有 $1+p$ 个非内交换的极大子群.

(3) G 至少有 p^2 个内交换的极大子群.

定理 14.9.32 设 G 是 $\mathcal{B}^*$ 群. 则

(1) $\Phi(G)\leqslant Z(G)$, $\Phi_{N\mathcal{A}_1M}(G)$ 交换.

(2) $G'\cong \mathrm{C}_p^2$ 或 $G'\cong \mathrm{C}_p^3$.

证明 (1) 由推论 14.9.31(3) 可设 A 和 B 是 G 的两个内交换的极大子群. 再由推论 14.9.31(1) 得 $d(G)=3$, 即 $|G:\Phi(G)|=p^3$, 由此可得 $\Phi(A)=\Phi(B)=\Phi(G)$. 又由定理 1.7.7 可知, $\Phi(A)=Z(A)$ 且 $\Phi(B)=Z(B)$. 由 $G=AB$ 推出 $\Phi(G)\leqslant Z(G)$. 再由推论 14.9.31(1) 可知, $\Phi(G)$ 是 $\Phi_{N\mathcal{A}_1M}(G)$ 的极大子群. 因而 $\Phi_{N\mathcal{A}_1M}(G)$ 交换.

(2) 由 $d(G)=3$ 和 $\Phi(G)\leqslant Z(G)$ 推出 $G'\leqslant \mathrm{C}_p^3$. 若 $G'\cong \mathrm{C}_p$, 则 $|G:Z(G)|=p^2$. 因而 $\Phi_{N\mathcal{A}_1M}(G)=Z(G)$. 又包含 $Z(G)$ 的极大子群是交换的, 其他的极大子群是内交换的. 因而 $G\in\mathcal{A}_2$. 这与 G 是 $\mathcal{B}^*$ 群的假设矛盾. □

由以上的分析可知, 分类 $\mathcal{B}$ 群可归结为分类 $\mathcal{B}^*$ 群. 由推论 14.9.31(3) 可知, $\mathcal{B}^*$ 群至少有 p^2 个内交换的极大子群. 又由推论 14.9.31 和定理 14.9.32 可知, $\mathcal{B}^*$ 群 G 满足如下条件:

$$d(G)=3,\quad \Phi(G)\leqslant Z(G),\quad G'\cong \mathrm{C}_p^2 \text{ 或 } \mathrm{C}_p^3.$$

值得庆幸的是, 至少有两个内交换极大子群的有限 p 群已被文献 [8],[9],[190] 分类. 因此依照 $G'\cong \mathrm{C}_p^2$ 或 C_p^3, 只需从中挑出满足上述条件的群并证明它们是 $\mathcal{B}^*$ 群即可. 分类结果可见文献 [267].

14.10 有限自对偶 p 群

设 G 是一个群. G 称为s **自对偶**(s-self dual), 若 G 的每个子群同构于 G 的一个商群. G 称为q **自对偶**(q-self dual), 若 G 的每个商群同构于 G 的一个子群. G 称为**自对偶**(self dual), 若 G 既是 s 自对偶的也是 q 自对偶的. 有限自对偶群首先是由 Spencer 在文献 [210] 发起研究的. 他证明的一个结果是如下定理.

定理 14.10.1 有限群 G 是自对偶的当且仅当 G 是幂零群且它的所有 Sylow 子群是自对偶的.

由定理 14.10.1 可知, 有限自对偶群的研究可归结为有限自对偶 p 群的研究. 一个自然的问题是: 有限自对偶 p 群的结构是如何的. 安立坚等在文献 [6] 首先确定了有限 s 自对偶 p 群的结构, 进而确定了有限自对偶 p 群的结构. 由此易得有限 s 自对偶群及有限自对偶群的结构. 李立莉等在文献 [122] 确定了有限内 s 自对偶群的结构, 作为副产品, 有限内自对偶群的结构也被确定. Janko 在文献 [105] 确定

了每个子群都是 q 自对偶的有限非交换 2 群, 在 $p>2$ 的情况下, 他在 $\Omega_1(G)$ 交换的假设下, 分类了每个子群都是 q 自对偶的有限非交换 p 群. 下面的两个定理就是文献 [105] 的主要结果.

定理 14.10.2 设 G 是非交换 2 群. 则 G 的子群都是 q 自对偶的当且仅当以下条件之一成立.

(a) G 为广义二面体群. 即 G 有一个方次数 >2 的交换极大子群 A 和一个 2 阶元 t 满足 $a^t=a^{-1}$ 对所有的 $a\in A$ 成立.

(b) $G=M\times V$, 其中 $M=\mathrm{M}_2(e,1)$, $e\geqslant 3$, 且 $\exp(V)\leqslant 2$.

定理 14.10.3 设 G 是非交换 p 群, $p>2$. 若 $\Omega_1(G)$ 交换, 则 G 的子群都是 q 自对偶的当且仅当以下条件成立.

$$G=M\times V,\quad \text{其中}\quad M=\mathrm{M}_p(n,1),\quad n\geqslant 2,\quad \text{且}\quad \exp(V)\leqslant p.$$

下面的内容主要是介绍有限 s 自对偶 p 群的结果. 取自 [6].

14.10.1 有限 s 自对偶 p 群的性质和例子

命题 14.10.4 设 G 是有限 s 自对偶 p 群.

(1) 若 $H\leqslant G$, 则 $d(H)\leqslant d(G)$;

(2) $\exp(G)=\exp(G/G')$;

(3) 若 K 是 G 的交换子群, 则 $|K|\leqslant|G/G'|$;

(4) 若 K 是 G 的交换子群且 $|K|=|G/G'|$, 则 $K\cong G/G'$;

(5) G/G_n 是 s 自对偶的;

(6) $G/\mho_1(G')$ 是 s 自对偶的.

证明 (1) 因为 G 是 s 自对偶的, H 与 G 的某个商群同构. 设 $H\cong G/N$. 则 $d(H)=d(G/N)\leqslant d(G)$.

(2) 取 $a\in G$ 使得 $o(a)=\exp(G)$. 因为 G 是 s 自对偶的, 故可设 $\langle a\rangle\cong G/N$. 于是 $G'\leqslant N$. 从而 $G/N\cong(G/G')/(N/G')$. 故 $\exp(G/N)\leqslant\exp(G/G')$. 于是

$$\exp(G)=o(a)=\exp(G/N)\leqslant\exp(G/G').$$

另一方面, $\exp(G/G')\leqslant\exp(G)$. 因而 $\exp(G)=\exp(G/G')$.

(3) 设 $K\cong G/N$. 则 $G'\leqslant N$. 因而 $|K|=|G/N|\leqslant|G/G'|$.

(4) 由 (3) 的证明即得.

(5) 设 $L/G_n\leqslant G/G_n$. 则 $L\leqslant G$. 设 $L\cong G/M$. 则 L/G_n 同构于 G/M 的某个商群. 设

$$L/G_n\cong(G/M)/(N/M)\cong G/N.$$

因为 $c(G/G_n) = n-1$, 故 $c(L/G_n) \leqslant n-1$. 由此可得 $c(G/N) \leqslant n-1$, 因而 $G_n \leqslant N$. 于是

$$L/G_n \cong G/N \cong (G/G_n)/(N/G_n).$$

由 L/G_n 的任意性可得, G/G_n 也是 s 自对偶的.

(6) 设 $L/\mho_1(G') \leqslant G/\mho_1(G')$. 则 $L \leqslant G$. 不妨设 $L \cong G/M$. 则 $L/\mho_1(G')$ 同构于 G/M 的某个商群. 设

$$L/\mho_1(G') \cong (G/M)/(N/M) \cong G/N.$$

因为 $\exp(G/\mho_1(G'))' = p$, 故 $\exp(L/\mho_1(G'))' = p$. 由此可得 $\exp(G/N)' = p$, 因而 $\mho_1(G') \leqslant N$. 于是

$$L/\mho_1(G') \cong G/N \cong (G/\mho_1(G'))/(N/\mho_1(G')).$$

由 $L/\mho_1(G')$ 的任意性可得, $G/\mho_1(G')$ 也是 s 自对偶的. □

引理 14.10.5 若 $H \times \langle a\rangle$ 是有限 s 自对偶 p 群, 则 H 的每个极大子群同构于 H 的某个商群.

证明 设 $G = H \times \langle a\rangle$, L 是 H 的一个极大子群. 则 $L \times \langle a\rangle$ 是 G 的一个极大子群. 因为 G 是 s 自对偶的, 故 $L \times \langle a\rangle$ 同构于 G 的某个商群. 设 $L \times \langle a\rangle \cong G/M$ 且 $|\langle a\rangle| = p^k$.

若 $M \leqslant H$, 则 $G/M \cong H/M \times \langle a\rangle$. 由 [241] 中的III, 定理 2.14 即得 $L \cong H/M$.

若 $M \nleqslant H$, 则 $M \bigcap H = 1$. 设 $G/M = T/M \times \langle bM\rangle$, 其中 $T/M \cong L$, $\langle bM\rangle \cong \langle a\rangle$. 于是 $G = T\langle b\rangle$, $|T| = |H|$, $(bM)^{p^k} = M$ 且 $[b, T] \in M$. 因为 $|G/H| = p^k$, 故 $b^{p^k} \in H$. 又由 $(bM)^{p^k} = M$ 可得 $b^{p^k} \in M$. 因而 $b^{p^k} \in H \bigcap M = 1$. 由此可得 $\langle b\rangle \cong \mathrm{C}_{p^k}$. 因为 $G' \leqslant H$, 故 $[b, T] \in H \bigcap M = 1$. 因而 $G = T \times \langle b\rangle$. 由 [241] 中的III, 定理 2.14 即得 $T \cong H$. 因为 $L \cong T/M$, 故 L 同构于 H 的某个商群. □

引理 14.10.6 若 $H \times \langle a\rangle$ 是有限 s 自对偶 p 群, 则 H 的每个子群同构于 H 的某个商群. 特别地, H 是 s 自对偶的.

证明 设 L 是 H 的一个真子群. 对 $|H : L|$ 作归纳. 令 K 是 H 的一个子群使得 $L \lessdot K$. 因为 $|H : K| < |H : L|$, 由归纳假设, K 同构于 H 的某个商群. 不妨设

$$K \cong H/N, \quad T/N \lessdot H/N, \quad T/N \cong L.$$

则 $T \lessdot H$. 由引理 14.10.5 可知, T 同构于 H 的某个商群. 不妨设 $T \cong H/P$. 因为 $L \cong T/N$, 故 L 同构于 H/P 的某个商群. 不妨设 $L \cong (H/P)/(M/P)$. 则 $L \cong H/M$. □

定理 14.10.7 若 $H \times M$ 是有限 s 自对偶 p 群, 其中 M 交换, 则 H 也是 s 自对偶的.

证明 因为 M 可表为循环群的直积, 由引理 14.10.6 即得结论. □

定义 14.10.8 一个群 G 称为**基本 s 自对偶**, 若 G 是 s 自对偶的, 且对 G 的每个真子群 H 均有 $H' < G'$.

定理 14.10.9 若 G 是有限 s 自对偶 p 群, H 是集 $\{H \mid H' = G'\}$ 的极小元, 则 $Z(G)$ 有一个子群 M 使得 $G = H \times M$. 进一步地, H 是基本 s 自对偶群.

证明 不妨设 $G/M \cong H$. 由

$$G' = H' \cong (G/M)' = G'M/M \cong G'/(M \bigcap G')$$

可得 $G' \bigcap M = 1$. 因为 $[M, G] \leqslant G' \bigcap M = 1$, 故 $M \leqslant Z(G)$.

由 H 的极小性可知, 对 G/M 的每个真子群 K/M 有 $(K/M)' < (G/M)'$. 也有

$$(HM/M)' = H'M/M \cong H'/(H' \bigcap M) \cong H' \cong (G/M)'.$$

因而 HM/M 不是 G/M 的真子群. 由此可得 $G = HM$. 因为

$$H \cong G/M = HM/M \cong H/(H \bigcap M),$$

这推出 $H \bigcap M = 1$. 因而 $G = H \times M$. 由定理 14.10.7 可得, H 是基本 s 自对偶群. □

下面给出两个有限非交换 s 自对偶 p 群的例子. 将证明: 有限非交换 s 自对偶 p 群恰是这两类 p 群.

定理 14.10.10 [210] 若 P 是有限 p 群, 则 P 的每个子群是自对偶的当且仅当 P 是交换的或 $P = H \times K$, 其中 H 是方次数为 p 的 p^3 阶超特殊群, K 是初等交换群.

下面的第一个例子直接由定理 14.10.10 给出.

例 14.10.11 若 $G = \mathrm{M}_p(1,1,1) \times \mathrm{C}_p^k$, 则 G 是自对偶的, 特别地, G 是 s 自对偶的.

例 14.10.12 设 $G = \mathrm{M}_p(n,n) \times M$ 是有限 p 群, 其中 M 交换且 $\exp(M) < p^n$. 则 G 是 s 自对偶的但不是 q 自对偶的.

为证明例 14.10.12, 先证下面的一个引理.

引理 14.10.13 设 $G = \mathrm{M}_p(n,n) \times M$ 是有限 p 群, 其中 M 交换且 $\exp(M) < p^n$. 若 $x, y \in G$ 使得 $[x, y] \neq 1$, 则 $\langle x, y\rangle \cong \mathrm{M}_p(n,n)$ 且 $G = \langle x, y\rangle \times M$.

证明 不妨设 $H = \mathrm{M}_p(n,n) = \langle a, b \mid a^{p^n} = b^{p^n} = 1, [a,b] = a^{p^{n-1}}\rangle$. 因为

$$Z(G) = Z(H) \times M = \langle a^p, b^p\rangle \times M,$$

由此推出 $G/Z(G) = \langle aZ(G), bZ(G)\rangle$ 是 p^2 阶初等交换群. 因为 $[x, y] \neq 1$, 故

$$x, y \notin Z(G), \quad \langle xZ(G), yZ(G)\rangle = \langle aZ(G),\ bZ(G)\rangle = G/Z(G).$$

因而 $\langle x, y\rangle{=}\langle az_1, bz_2\rangle$, 其中 $z_1, z_2 \in Z(G)$. 不妨设 $x{=}az_1$, $y{=}bz_2$. 因为 $\exp(Z(G)) < p^n$, 故

$$[x, y] = [az_1, bz_2] = a^{p^{n-1}} = x^{p^{n-1}}.$$

因而

$$\langle x, y\rangle = \langle x, y \mid x^{p^n} = y^{p^n} = 1, [x, y] = x^{p^{n-1}}\rangle \cong \mathrm{M}_p(n, n).$$

观察到

$$\Omega_1(\langle x, y\rangle) = \langle x^{p^{n-1}},\ y^{p^{n-1}}\rangle = \langle a^{p^{n-1}},\ b^{p^{n-1}}\rangle,$$

$$\Omega_1(\langle x, y\rangle \bigcap M) \leqslant \Omega_1(\langle x, y\rangle) \bigcap M = \langle a^{p^{n-1}}, b^{p^{n-1}}\rangle \bigcap M = 1.$$

由此可得 $\langle x, y\rangle \bigcap M = 1$. 因而 $G = \langle x, y\rangle \times M$. □

例 14.10.12 的证明 我们有 $Z(G){=}Z(H){\times}M$. 由此可得 $G/Z(G) \cong H/Z(H)$ 是 p^2 阶的初等交换群. 因为 $Z(G)$ 是含在 G 的每个极大子群中, 故存在由 G 的极大交换子群组成的集合到 $G/Z(G)$ 的极大子群组成的集合之间的一个双射. 因而 G 有 $1+p$ 个极大交换子群. 设

$$H = \langle a, b \mid a^{p^n} = b^{p^n} = 1, [a, b] = a^{p^{n-1}}\rangle.$$

则 G 的极大交换子群分别是 $\langle a^p\rangle{\times}\langle b\rangle{\times}M$ 和 $\langle b^p\rangle{\times}\langle ab^i\rangle{\times}M$, 其中 $i = 0, 1, \cdots, p{-}1$. 它们中的每一个同构于 G/G'. 下证 G 的每个真子群 L 同构于 G 的某个商群.

若 L 交换, 则存在 G 的极大交换子群 K 使得 $L \leqslant K$. 上面的证明表明 $K \cong G/G'$. 定理 14.10.10 给出 K 是自对偶的. 因而 L 同构于 K 的某个商群. 于是 L 同构于 G/G' 的某个商群. 不妨设 $L \cong (G/G')/(N/G')$. 则 $L \cong G/N$.

若 L 非交换, 则存在 $x, y \in L$ 使得 $[x, y] \neq 1$. 由引理 14.10.13 可得, $G = \langle x, y\rangle \times M$. 于是

$$L = L\bigcap G = L\bigcap(\langle x, y\rangle \times M) = \langle x, y\rangle \times (L\bigcap M).$$

因为 M 交换, 定理 14.10.10 给出 M 是自对偶的. 于是 $L\bigcap M$ 同构于 M 的某个商群. 不妨设 $L\bigcap M \cong M/N$. 则

$$L = \langle x, y\rangle \times (L\bigcap M) \cong (\langle x, y\rangle \times M)/N = G/N.$$

最后证明 G 不是 q 自对偶的. 设 $N = \langle b^p\rangle \times M$. 则 $G/N \cong \mathrm{M}_p(n, 1)$. 由引理 14.10.13 可知, G 的任意两个非交换元素生成 $\mathrm{M}_p(n, n)$. 由此可知, 不存在 G 的子群同构于 G/N. 故 G 不是 q 自对偶的. □

在本节的最后, 给出二元生成的有限 s 自对偶 p 群的结构. 由命题 14.10.4 (1) 可知, 若 G 为二元生成的有限 s 自对偶 p 群, 则 G 的所有子群都是二元生成的. 而后者已经在文献 [31] 中被分类. 定理 8.2.3 给出了这个分类结果. 对定理 8.2.3 中的群检验之后可得下面的结论.

定理 14.10.14　设 G 是二元生成的有限非交换 p 群. 则 G 是 s 自对偶的当且仅当 G 同构于 $\mathrm{M}_p(n,n)$ 或 $\mathrm{M}_p(1,1,1)$, 其中 $p>2$.

14.10.2　有限 s 自对偶 p 群的分类

本节先决定导群初等交换的 s 自对偶 p 群. 为此, 需要一个关于斜对称的双线性映射的引理.

引理 14.10.15　设 $V=V(n,\mathbb{F})$ 是域 $\mathbb{F}$ 上的 n 维向量空间, $T=(k,\mathbb{F})$ 是域 $\mathbb{F}$ 上的 k 维线性空间. $f:V\times V\longrightarrow T$ 是一个斜对称的双线性映射, 即对任意的 $u,v,w\in V$. $a\in\mathbb{F}$, 有

(i) $f(au,v)=f(u,av)=af(u,v)$;

(ii) $f(u+w,v)=f(u,v)+f(w,v), f(u,v+w)=f(u,v)+f(u,w)$;

(iii) $f(u,u)=0$,

且 $f(V\times V)$ 生成 T, 则

(1) 存在 V 的子空间 S 使得 $f(S\times S)$ 也生成 T, 且 S 的维数不超过 $k+1$.

(2) 设 $k\geqslant 2$, S 是 V 的 $k+1$ 维子空间, 满足 $f(S\times S)$ 也生成 T, 并且对于 S 的任意真子空间 R 都有 $f(R\times R)$ 生成 T 的真子空间. 则存在 S 的 2 维子空间 A 使得 $f(A\times A)$ 为零空间.

证明　(1) 对 k 用数学归纳法. 设 T_1 是 T 的一个 $k-1$ 维子空间, 则存在 $u,v\in V$ 使得 $f(u,v)\notin T_1$.

再设 j_1 是 T 到 T_1 的投射, 则容易验证 $j_1f:V\times V\longrightarrow T_1$ 仍是一个双线性映射, 且 $j_1f(V\times V)$ 生成 T_1. 因为 T_1 的维数为 $k-1$, 故存在 V 的子空间 S_1 使得 $j_1f(S_1\times S_1)$ 也生成 T_1, 且 S_1 的维数不超过 k. 若 $f(S_1\times S_1)$ 生成 T, 则 S_1 即为满足条件的 S, 因此不妨设 $f(S_1\times S_1)$ 生成 T_1. 若 S_1 的维数小于 k, 取 S 为 S_1,u,v 生成的子空间即可满足条件, 因此又不妨设 S_1 的维数为 k.

再设 T_2 是 T_1 的一个 $k-2$ 维子空间, j_2 是 T 到 T_2 的投射. 则 $j_2f:S_1\times S_1\longrightarrow T_2$ 也是一个双线性映射, 且 $j_2f(S_1\times S_1)$ 生成 T_2. 因为 T_2 的维数为 $k-2$, 故存在 S_1 的子空间 S_2 使得 $j_2f(S_2\times S_2)$ 也生成 T_2, 且 S_2 的维数不超过 $k-1$. 取 S_3 为 S_1 中包含 S_2 的 $k-1$ 维子空间. 则 $f(S_3\times S_3)$ 生成 T_2 或 T_1. 若 $f(S_3\times S_3)$ 生成 T_1, 取 S 为 S_3,u,v 生成的子空间即可满足条件. 因此又不妨设 $f(S_3\times S_3)$ 生成 T_2.

若存在 $\alpha\in S_1$ 使得 $f(\alpha,u)\notin T_1$ 或者 $f(\alpha,v)\notin T_1$, 取 S 为 S_1,u 生成的子空间或者 S_1,v 生成的子空间, 则 S 满足条件. 因此不妨再设 $f(\alpha,u)\in T_1$ 和 $f(\alpha,v)\in T_1$

对所有的 $\alpha \in S_1$ 成立.

设 S_1 为 S_3 和 α_1 生成的. 因为 f 是斜对称的, 故存在 $\alpha_2 \in S_3$ 使得 $w = f(\alpha_2, \alpha_1) \notin T_2$, 从而 $T_1 = T_2 \oplus L(w)$. 设 $f(\alpha_2, u) = iw + t$, 其中 $t \in T_2$. 取 S 为 $S_3, (1-i)\alpha_1 u$ 和 v 生成的子空间. 因为 $f(\alpha_2, (1-i)\alpha_1 u) = w + t$, 故 $f(S \times S)$ 生成的空间包含 T_1. 又 $f((1-i)\alpha_1 u, v) \notin T_1$, 故 $f(S \times S)$ 生成整个空间 T.

(2) 假设结论不成立. 首先断言: 对于 S 的任何一组基 $a_1, a_2, \cdots, a_{k+1}$ 有

$$f(a_1, a_2), f(a_1, a_3), \cdots, f(a_1, a_{k+1}) \text{ 线性无关.}$$

若否, 则存在不全为零的元素 $j_2, j_3, \cdots, j_{k+1}$ 使得

$$j_2 f(a_1, a_2) + j_3 f(a_1, a_3) + \cdots + j_{k+1} f(a_1, a_{k+1}) = 0.$$

令

$$A = L(a_1, j_2 a_2 + j_3 a_3 + \cdots + j_{k+1} a_{k+1}).$$

由于 $f(a_1, j_2 a_2 + j_3 a_3 + \cdots + j_{k+1} a_{k+1}) = 0$, 故 A 是满足 $f(A \times A)$ 为零空间的 S 的 2 维子空间, 与假设矛盾.

设 $S = L(a_1, a_2, \cdots, a_{k+1})$. 由以上断言可知

$$T = L(f(a_1, a_2), f(a_1, a_3), \cdots, f(a_1, a_k)) \oplus L(f(a_1, a_{k+1})).$$

同理, $T = L(f(a_2, a_1), f(a_1, a_3), \cdots, f(a_2, a_k)) \oplus L(f(a_2, a_{k+1}))$.

记

$$M = L(f(a_1, a_2), f(a_1, a_3), \cdots, f(a_1, a_k)),$$
$$N = L(f(a_2, a_1), f(a_2, a_3), \cdots, f(a_2, a_k)).$$

若 $M \neq N$, 令 $R = L(a_1, a_2, \cdots, a_k)$, 则 $f(R \times R)$ 生成 T, 与题设矛盾. 因此, 一定有 $M = N$.

设

$$f(a_2, a_{k+1}) = i f(a_1, a_{k+1}) + m,$$

其中 $m \in M$, 则 $f(a_2 - i a_1, a_{k+1}) = m \in M$. 令

$$a_2' = a_2 - i a_1,\ N' = L(f(a_2', a_1), f(a_2', a_3), \cdots, f(a_2', a_k))$$

则仍有 $M = L(f(a_1, a_2'), f(a_1, a_3), \cdots, f(a_1, a_k))$ 和 $N' = M$. 因为 $f(a_2', a_{k+1}) \in M = N'$, 故 $f(a_2', a_1), f(a_2', a_3), \cdots, f(a_2', a_{k+1})$ 线性相关, 与上面的断言矛盾. □

定理 14.10.16 设 G 为有限 p 群, $c(G) = 2$ 且 $G' \cong C_p^k$, 则存在 G 的子群 K 满足 $K' = G'$ 且 $d(K) \leqslant k + 1$.

证明 因为 $G' \cong C_p^k$, 所以 G' 可以看作域 $\mathrm{GF}(p)$ 上的 k 维线性空间. 令 $\overline{G} = G/\Phi(G)$, 则 $\overline{G}$ 也可以看作域 $\mathbb{F}_p$ 上的线性空间. 建立 $\overline{G} \times \overline{G}$ 到 G' 的映射 f, 满足对任意的 $\overline{g}, \overline{h} \in \overline{G}$, 有 $f(\overline{g}, \overline{h}) = [g, h]$, 则由 $c(G) = 2$ 可知 f 是一个斜对称的双线性映射. 由引理 14.10.15(1) 可知, 存在 $\overline{G}$ 的子空间 $\overline{K}$ 使得 $f(\overline{K}, \overline{K})$ 生成 G', 并且 $\overline{K}$ 的维数不超过 $k+1$. 设 $\overline{K} = L(\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_s)$, 其中 $s \leqslant k+1$. 令 $K = \langle x_1, x_2, \cdots, x_s \rangle$, 则 $K' = G'$, 并且 $d(K) \leqslant k+1$. □

引理 14.10.17 设 G 为类 2 的基本的 s 自对偶 p 群, $\exp(G') = p$, 则 $|G'| = p$.

证明 因为 $c(G) = 2$, 故 $G' \leqslant Z(G)$ 且 G' 是初等交换 p 群. 设 $|G'| = p^k$. 则由题设及定理 14.10.16 可知 $d(G) \leqslant k+1$. 又由命题 14.10.4(1) 可知 $d(G) \geqslant d(G') = k$, 从而 $d(G) = k$ 或 $k+1$.

若 $d(G) = k$, 设 a 是 G 的一个最高阶元. 由 G 是 s 自对偶可知, 存在 G 的正规子群 N 使得 $G/N \cong \langle a \rangle$. 设 $G/N = \langle bN \rangle$. 则 b 也是 G 的一个最高阶元且 $\langle b \rangle \bigcap N = 1$. 由于 $G' \leqslant N$, 故 $\langle b \rangle \bigcap G' = 1$. 因此 $\langle b, G' \rangle = G' \times \langle b \rangle$ 为 $k+1$ 元生成的交换群. 这与命题 14.10.4(1) 矛盾.

若 $d(G) = k+1$, 下面证明 $k=1$. 若否, $k \geqslant 2$. 因为 $G' \cong C_p^k$, 故 G' 可以看作域 $\mathrm{GF}(p)$ 上的 k 维线性空间. 令 $\overline{G} = G/\Phi(G)$. 则 $\overline{G}$ 也可以看作域 $\mathrm{GF}(p)$ 上的线性空间. 建立 $\overline{G} \times \overline{G}$ 到 G' 的映射 f, 满足对任意的 $\bar{g}, \bar{h} \in \overline{G}$, 有 $f(\bar{g}, \bar{h}) = [g, h]$. 则由 $c(G) = 2$ 可知, f 是一个斜对称的双线性映射. 由引理 14.10.15(2) 可知, 存在 $\overline{G}$ 的 2 维子空间 $\overline{A}$ 使得 $f(\overline{A}, \overline{A})$ 为零空间. 设 $\overline{A} = L(\bar{x}_1, \bar{x}_2)$. 令 $A = \langle x_1, x_2, \Phi(G) \rangle$. 因为 $|G/A| = p^{k-1}$, 故 $|A| = \dfrac{|G|}{p^{k-1}}$. 又由 $c(G) = 2$ 和 $\exp(G') = p$ 可知 $\Phi(G) \leqslant Z(G)$. 所以 A 交换. 但是

$$|A| = \frac{|G|}{p^{k-1}} > \frac{|G|}{p^k} = |G/G'|.$$

这与命题 14.10.4(4) 矛盾. 因此一定有 $k = 1$, 即 $|G'| = p$. □

推论 14.10.18 设 G 为类 2 的有限 s 自对偶 p 群, $\exp(G') = p$. 则 $|G'| = p$.

证明 由定理 14.10.9 可知, G 能分解为一个基本的 s 自对偶群 H 和一个交换群 M 的直积. 由引理 14.10.17 可知, $|H'| = p$, 从而 $|G'| = p$. □

引理 14.10.19 设 G 是有限 s 自对偶 p 群, $\exp(G') = p$. 则 $|G'| = p$.

证明 由推论 14.10.18, 只需证 $c(G) = 2$. 若否, 设 G 是极小阶反例. 则 G 一定是基本的 s 自对偶 p 群. 又由命题 14.10.4 (5) 可知 $c(G) = 3$.

令 $\overline{G} = G/G_3$. 则 $c(\overline{G}) = 2$. 由命题 14.10.4 (5) 可知 $\overline{G}$ s 自对偶. 因为 $\exp(G') = p$, 故 $\exp(\overline{G}') = p$. 由推论 14.10.18 可知, $|\overline{G}'| = p$. 设 $\overline{G}' = \langle [\overline{a}, \overline{b}] \rangle$. 则由引理 14.10.9 可设

$$\overline{G} = \langle \overline{a}, \overline{b} \rangle \times \langle \overline{c}_1 \rangle \times \cdots \times \langle \overline{c}_t \rangle.$$

从而又可设 $G=\langle a,b,c_1,c_2,\cdots,c_t\rangle$. 由于 $|G'/G_3|=|\overline{G}'|=p$, 可设 $G'=\langle [a,b],G_3\rangle$. 从而

$$G_3=[G',G]=\langle [b,a,c_i],[b,a,a],[b,a,b]\rangle.$$

因为 $[a,c_i]\in G_3\leqslant Z(G)$, 故 $[a,c_i,b]=1$. 同理 $[c_i,b,a]=1$. 由命题 1.1.8(4) 可得 $[b,a,c_i]=1$, 即 $G_3=\langle [b,a,a],\ [b,a,b]\rangle$. 令 $S=\langle a,b\rangle$. 则 $S'=G'$. 因为 G 是基本的 s 自对偶 p 群, 故 $G=S=\langle a,b\rangle$. 由定理 14.10.14 可知, G 为 $\mathrm{M}_p(n,n)$ 或 $\mathrm{M}_p(1,1,1)$, 其中 $p>2$. 与 $c(G)=3$ 矛盾. 因此假设不成立. □

接下来将定出导群初等交换的 s 自对偶 p 群的结构.

定理 14.10.20 设 G 为导群初等交换的 s 自对偶 p 群. 则 G 同构于以下群之一:

(1) $\mathrm{M}_p(1,1,1)\times \mathrm{C}_p^n$, 其中 $p>2$;

(2) $\mathrm{M}_p(n,n)\times M$, 其中 M 交换且 $\exp(M)<p^n$.

证明 由引理 14.10.19 可知 $|G'|=p$. 设 H 是 G 的内交换子群. 则 $H'=G'$ 且对于 H 的真子群 K 都有 $K'<H'$. 因此, 由定理 14.10.9 可设 $G=H\times M$, 其中 M 是交换群. 而且还有 H 是基本的 s 自对偶 p 群. 由定理 14.10.14 可知, H 是 $\mathrm{M}_p(n,n)$, 或 $\mathrm{M}_p(1,1,1)$, 其中 $p>2$. 从而要决定所有的导群初等交换的 s 自对偶 p 群, 只需从群 $\mathrm{M}_p(1,1,1)\times M$ 和群 $\mathrm{M}_p(n,n)\times M$ (其中 M 交换) 中取出满足 s 自对偶条件的群即可.

(1) $G\cong \mathrm{M}_p(1,1,1)\times M$.

下面证明 G 是 s 自对偶的当且仅当 $\exp(M)\leqslant p$.

由定理 14.10.10 可知充分性成立. 下面证明必要性.

取 $c\in M$ 使 $o(c)=\exp(M)$, 考虑 G 的内交换子群 $A=\langle ac,b\rangle$. 则 A 是 G 的满足 $A'=G'$ 的极小的子群, 由定理 14.10.9 可知, 存在 G 的交换正规子群 N, 使得 $G=A\times N$. 由 [241] 中的定理 4.7 可知, $A\cong \mathrm{M}_p(1,1,1)$. 因此 $\exp(M)\leqslant p$.

(2) $G\cong \mathrm{M}_p(n,n)\times M$.

我们下面证明 G 是 s 自对偶的当且仅当 $\exp(M)<p^n$.

由例 14.10.12 的证明可知充分性成立. 下面证明必要性.

取 $c\in M$ 使得 $o(c)=\exp(M)$. 考虑 G 的内交换子群 $H=\langle ac,b\rangle$. 则 H 是 G 的满足 $H'=G'$ 的极小的子群. 由引理 14.10.9 可知, 存在 G 的交换正规子群 L 使得 $G=H\times L$. 由 [241] 中的III, 定理 2.14 可知,

$$H=\langle ac,b\rangle\cong\langle a,b\rangle\cong \mathrm{M}_p(n,n).$$

由 $\exp(H)=\exp(\mathrm{M}_p(n,n))=p^n$ 可得 $o(c)\leqslant p^n$, 从而 $\exp(M)\leqslant p^n$. 若 $\exp(M)=p^n$, 则

$$H=\langle ac,b\mid (ac)^{p^n}=b^{p^n}=1,[ac,b]=a^{p^{n-1}}\rangle\cong \mathrm{M}_p(n,n,1).$$

矛盾. 因此, 一定有 $\exp(M) < p^n$.

综上(1),(2)可知, 导群初等交换的 s 自对偶 p 群 G 只能是 $\mathrm{M}_p(n,n) \times M$ 或 $\mathrm{M}_p(1,1,1) \times \mathrm{C}_p^n$, $p > 2$, 其中 M 交换, $\exp(M) < p^n$. □

现在可以确定出所有的 s 自对偶 p 群. 由下述定理的论证可知, 不存在导群非初等交换的 s 自对偶 p 群,

定理 14.10.21　设 G 为有限非交换的 s 自对偶 p 群, 则 G 同构于以下群之一.

(1) $\mathrm{M}_p(1,1,1) \times \mathrm{C}_p^n$, 其中 $p > 2$;

(2) $\mathrm{M}_p(n,n) \times M$, 其中 M 交换且 $\exp(M) < p^n$.

证明　设 H 是一个极小的满足 $H' = G'$ 的 G 的子群. 由定理 14.10.9 可设 $G = H \times M$, 其中 M 是一个交换群. 并且我们还知道 H 是一个基本的 s 自对偶 p 群. 由命题 14.10.4 (6) 可知, $H/\mho_1(H')$ 也是 s 自对偶. 又因为

$$\exp(H/\mho_1(H'))' = \exp(H'/\mho_1(H')) = p,$$

由引理 14.10.19 可知,

$$|(H/\mho_1(H'))'| = |H'/\mho_1(H')| = p.$$

从而 H' 循环. 进而存在 $a, b \in H$ 使得 $\langle [a,b] \rangle = H'$. 由 H 的极小性可知 $H = \langle a, b \rangle$. 又由定理 14.10.14 可知, $|H'| = p$. 最后由定理 14.10.20 可知结论成立. □

14.11　p 群的 Wielandt 列和 Norm

回顾一下, 群 G 的 Wielandt 子群就是 G 的所有次正规子群的正规化子的交, 记为 $w(G)$. Wielandt[232] 证明了对于有限群 G, $w(G)$ 是 G 的非平凡的特征子群. 他还如下定义了一个终止于 G 的正规子群列: 令 $w_0(G) = 1$, 对于 $i \geqslant 0$, $w_{i+1}(G)/w_i(G) = w(G/w_i(G))$. 这样的子群列通常称为 Wielandt 列, 使得 $w_n(G) = G$ 的最小数 n 称为 G 的 Wielandt 长. 另一个相关的概念就是 Baer[15] 引进的群 G 的 Norm. 它被定义为 G 的所有子群的正规化子的交, 记为 $N(G)$. 显然, $Z(G) \leqslant N(G)$. 对于幂零群 G 而言, $w(G) = N(G)$. Schenkman[198] 证明了对于任意的群 G, G 的 Norm 含在 G 的 2 中心里, 即 $N(G) \leqslant Z_2(G)$. 于是 $N(G)$ 与上中心群列之间就有一个有趣的关系:

$$Z(G) \leqslant N(G) \leqslant Z_2(G).$$

一个自然的问题是: $Z(G) = N(G)$ 的群是什么样子呢? $N(G) = Z_2(G)$ 的群又是什么样子呢? 郭秀云等在文献 [75] 研究了这个问题. 本节介绍他们的结果.

另一个自然的问题是: 幂零群的 Wielandt 列与上中心群列之间有什么关系. Bryce 和 Cossey 在文献 [43] 证明了对于方次数不超过 p^2, 幂零类充分大的亚交换 p 群, Wielandt 列与上中心群列一致. Ormerod 研究了 p 群的幂零类是如何被 Wielandt 长控制的等, 见文献 [173]—[177]. 张小红等在文献 [282] 研究了极大类 p 群的 Wielandt 列和上中心群列之间的关系. 本节介绍他们的结果.

为方便, 本节和 14.12 节用 $N(G:H)$ 和 $w(G:H)$ 分别表示 $N(G/H)$ 和 $w(G/H)$ 在 G 中的原像. α: $G\to G/H$ 表示自然同态. 以下内容取自 [75].

引理 14.11.1 设 G 是群, $H\leqslant Z(G)$. 则对于 $g,h\in G$, $n\in N(G:H)$ 有

(1) $[g,n,h]$, $[h,n,g]$, $[g,h,n]\in Z(G)$;

(2) $[n,g,g]=1$, $[n,g^{-1}]=[n,g]^{-1}$;

(3) $[g,n,h][h,n,g]=1$;

(4) 若 $N(G)=Z_2(G)$, 则 $[g,n,h]\in Z(G)\bigcap\langle g\rangle\bigcap\langle h\rangle$.

证明 (1) 由 [198] 可知, $N(G/H)\leqslant Z_2(G/H)\leqslant Z_3(G)/H$. 从而 $n\in Z_3(G)$. 于是 $[g,n,h]$, $[h,n,g]$, $[g,h,n]\in Z(G)$.

(2) 令 $\overline{G}=G/H$. 对于 $\bar{n}\in N(\overline{G})$, $\bar{g}\in\overline{G}$, 有 $\bar{g}^{\bar{n}}=\bar{g}^i$, 其中 i 是正整数. 这意味着 $g^n\equiv g^i(\mathrm{mod}\ H)$. 从而 g^n 与 g 交换. 于是

$$1=[g^n,g]=[g[g,n],g]=[g,n,g]=[n,g,g],\quad [n,g^{-1}]=[n,g]^{-1}.$$

(3) 由 (2) 即得

$$[gh,n]^{gh}=[gh,n]=[g,n][h,n][g,n,h].$$

另一方面,

$$[gh,n]^{gh}=([gh,n]^g)^h=([g,n][h,n][h,n,g][g,n,h])^h=[g,n][g,n,h]^2[h,n][h,n,g].$$

于是 $[g,n,h][h,n,g]=1$.

(4) 因为 $n\in Z_3(G)$, 故 $[g,n],[h,n]\in Z_2(G)=N(G)$. 于是 $[g,n,h]\in\langle h\rangle$ 且 $[h,n,g]\in\langle g\rangle$. 由 (3) 得, $[g,n,h]=[h,n,g]^{-1}$. 由此推出 $[g,n,h]\in Z(G)\bigcap\langle g\rangle\bigcap\langle h\rangle$. □

引理 14.11.2 设 G 是群, $H\leqslant Z(G)$ 且 $n\in N(G:H)$. 若对 $i=1,2,\cdots,k;j=1,2,\cdots,m$ 有 $[g_i,n,h_j]=1$, 则

$$\left[\prod_{i=1}^{k}g_i,n,\prod_{j=1}^{m}h_j\right]=1.$$

证明　对 $m+k$ 作归纳. 若 $m+k=2$, 由假设即得 $[g_1,n,h_1]=1$. 若 $k>m=1$, 由 14.11.1(3) 和归纳假设得

$$\left[\prod_{i=1}^{k} g_i, n, h_1\right] = \left[h_1, n, \prod_{i=1}^{k} g_i\right]^{-1} = [h_1, n, g_k]^{-1}\left[h_1, n, \prod_{i=1}^{k-1} g_i\right]^{-1} = 1.$$

若 $m \geqslant 2$, 由归纳得

$$\left[\prod_{i=1}^{k} g_i, n, \prod_{j=1}^{m} h_j\right] = \left[\prod_{i=1}^{k} g_i, n, h_m\right]\left[\prod_{i=1}^{k} g_i, n, \prod_{j=1}^{m-1} h_j\right] = 1. \qquad \square$$

引理 14.11.3　*设 G 是奇数阶正则 p 群, $n \in N(G)$. 则*

(1) 若对 $h \in G$ 有 $o(h)=\exp(G)$ 且 $h^n=h^i$, 则对所有的 $g \in G$ 有 $g^n=g^i$, 其中 i 是正整数;

(2) $N(G)/Z(G)$ 循环;

(3) 令 $N(G)=\langle a\rangle Z(G)$. 则对 $g \in G$ 有 $g^a=g^{1+p^{m-k}}$, 其中 $\exp(G)=p^m$ 且 $\exp(N(G)/Z(G))=p^k$.

证明　(1) 因为 $N(G)$ 的元在 G 上诱导一个幂自同构, 故对所有的 $g \in G$, 存在整数 m 使得对所有的 $g \in G$ 都有 $g^n=g^m$. 若 $o(h)=\exp(G)$ 且 $h^n=h^i$, 则 $i \equiv m(\mathrm{mod}\ \exp(G))$. 于是对所有的 $g \in G$ 有 $g^n=g^i$.

(2) 若 G 是正则 p 群, 则每个幂自同构是平凡的, 且经限制同态, 对 G 的每个极大阶的循环子群 $\langle x\rangle$, $\mathrm{PAut}(G)$ 可嵌入到 $\mathrm{Aut}(\langle x\rangle)$ 中. 因为 $N(G)$ 的元在循环群 $N(G)/Z(G) \lesssim \mathrm{PAut}(G) \lesssim \mathrm{Aut}(\langle x\rangle)$ 上诱导一个幂同构, 因而 $N(G)/Z(G)$ 循环.

(3) 若 $N(G)=Z(G)$, 结论显然成立. 若 $N(G)\neq Z(G)$, 不妨设$N(G)=\langle a_1\rangle Z(G)$. 则存在 $h \in G$ 使得 $o(h)=p^m$ 且 $h^{a_1}=h^i$, 其中 i 是正整数且 $i \not\equiv 1(\mathrm{mod}\ p^m)$. 注意到 $o(a_1Z(G))=p^k$. 则 $i^{p^k} \equiv 1(\mathrm{mod}\ p^m)$. 故 $i=1+jp^{m-k}$, 其中 $(j,p)=1$. 令 $a=a_1^t$ 使得 $(1+jp^{m-k})^t \equiv 1+p^{m-k}(\mathrm{mod}\ p^m)$. 则 $h^a=h^{1+p^{m-k}}$. 不妨设 $N(G)=\langle a\rangle Z(G)$. 则对 $g \in G$, 由 (1) 得 $g^a=g^{1+p^{m-k}}$. $\square$

引理 14.11.4　*设 G 是正则 p 群. 若下列之一成立, 则 $N(G)=Z(G)$.*

(1) 存在 $g \in G$ 使得 $o(g)=\exp(G)$ 且 $\langle g\rangle \bigcap G'=1$;

(2) 存在 $g \in G$ 使得 $o(g)=\exp(G)$ 且 $Z_2(G) \leqslant C_G(g)$;

(3) $\exp(G)=\exp(G')$.

证明　(1) 对 $n \in N(G)$ 有 $g^n=g[g,n] \in \langle g\rangle$. 因为 $\langle g\rangle \bigcap G'=1$, 故 $[g,n]=1$. 从而 $g^n=g$. 对所有的 $h \in G$, 由引理 14.11.3(1) 推出 $h^n=h$. 因而 $N(G)=Z(G)$.

(2) 因为 $N(G) \leqslant Z_2(G) \leqslant C_G(g)$, 故对 $n \in N(G)$ 有 $g^n=g$. 对所有的 $h \in G$, 由引理 14.11.3(1) 推出 $h^n=h$. 因而 $N(G)=Z(G)$.

(3) 选择 $g \in G'$ 使得 $o(g) = \exp(G')$. 由 $[G', Z_2(G)] = 1$ 推出 $Z_2(G) \leqslant C_G(g)$. 由 (2) 得 $N(G) = Z(G)$. □

引理 14.11.5 设 G 是奇阶 p 群. 令 $G' = \langle c \rangle$. 若 c 是 G 的唯一性基的元, 则 $N(G) = Z(G)$.

证明 因为 G' 循环, G 是正则 p 群. 设 $(a_1, a_2, \cdots, c, \cdots, a_n)$ 是 G 的唯一性基, 其中 $o(a_1) = \exp(G)$. 则 $\langle c \rangle \bigcap \langle a_1 \rangle = 1$ 或 $a_1 = c$. 由引理 14.11.4 推出 $N(G) = Z(G)$. □

引理 14.11.6 设 G 是内交换 p 群, 如定理 1.7.10所设. 则

(1) 若 $G \cong \mathrm{Q}_8$, 则 $N(G) = Z_2(G)$;

(2) 若 $G \cong \mathrm{M}_p(n, m, 1)$, 则 $N(G) = Z(G)$;

(3) 若 $G \cong \mathrm{M}_p(n, m)$, 则对 $n \leqslant m$ 有 $N(G) = Z(G)$, 对 $n > m$ 且 G 不是 D_8 有 $N(G) = \langle a^p, b \rangle$, 对 $G \cong \mathrm{D}_8$ 有 $N(G) = Z(G)$.

证明 证明留给读者. □

定理 14.11.7 设 G 是 Capable 群. 不妨设 $G \cong H/Z(H)$. 若下列之一成立, 则 $N(G) = Z(G)$.

(i) $H' \bigcap Z_2(H)$ 的每个子群在 H 中正规;

(ii) $N(H) = Z_2(H)$ 且 $|Z(H)|$ 无平方因子;

(iii) H 是正则 p 群且 $N(H) = Z_2(H)$.

证明 设 $N(H/Z(H)) \neq Z(H/Z(H))$. 则存在 $n \in N(H : Z(H))$ 和 $g,\ h \in H$ 使得 $[g, n, h] \neq 1$. 由引理 14.11.2, 不妨设 g 和 h 的阶是素数幂. 令 $o(g) = p^k$ 且 $o(h) = q^l$. 则由引理 14.11.1(2), $o([g, n])$ 是 p 的幂且 $o([h, n])$ 是 q 的幂.

(i) 因为 $[g, n] \in H' \bigcap Z_2(H)$, 故 $\langle [g, n] \rangle \trianglelefteq H$. 从而 $[g, n, h] \in \langle [g, n] \rangle$. 类似地, $[h, n, g] \in \langle [h, n] \rangle$. 由引理 14.11.1(3) 得, $[g, n, h] \in \langle [g, n] \rangle \bigcap \langle [h, n] \rangle$. 因而 $p = q$ 且 $\langle [g, n] \rangle \bigcap \langle [h, n] \rangle \neq 1$.

选择 $g,\ h$ 使得 $[g, n, h] \neq 1$ 且 $[g, n]$ 的阶极小, 不妨设 p^k. 由 $[g, n, h][h, n, g] = 1$ 推出 $o([g, n]) \leqslant o([h, n])$. 不妨设 $[g, n]^{p^{k-1}} = [h, n]^{up^{k-1}}$, 其中 u 是整数且 $k \geqslant 2$. (若 $k = 1$, 则 $[g, n] \in \langle [h, n] \rangle$. 从而 $[g, n, h] = 1$. 矛盾.) 由 $o([g, n])$ 的极小性可得

$$[g^p, n, h] = [[g, n]^p, h] = [g, n, h]^p = 1.$$

故 $o([g, n, h]) = p$. 令 $g_1 = gh^{-u}$. 则

$$\begin{aligned}
[g_1, n]^{p^{k-1}} &= [gh^{-u}, n]^{p^{k-1}} \\
&= ([g, n][g, n, h^{-u}][h, n]^{-u})^{p^{k-1}} && (\text{因为 } [[h, n], h] = 1) \\
&= [g, n]^{p^{k-1}} [g, n, h]^{-up^{k-1}} [h, n]^{-up^{k-1}} && (\text{因为 } [G', Z_2(G)] = 1) \\
&= [g, n]^{p^{k-1}} [h, n]^{-up^{k-1}} = 1.
\end{aligned}$$

因而 $o([g_1,n]) \leqslant p^{k-1}$. 但是

$$\begin{aligned}[g_1,n,h]&=[gh^{-u},n,h]=[[g,n]^{h^{-u}}[h^{-u},n],h]\\&=[[g,n][g,n,h^{-u}][h^{-u},n],h]=[g,n,h]\neq 1.\end{aligned}$$

与 $o([g,n])$ 的极小性矛盾.

(ii) 由引理 14.11.1(4) 得, $[g,n,h]\in Z(H)\bigcap\langle g\rangle\bigcap\langle h\rangle$. 因而 $p=q$ 且 $o([g,n,h])=p$. 令 $\overline{H}=H/Z(H)$. 则 $\bar{g}^{\bar{n}}=\bar{g}^i$, 其中 i 是正整数且 $(i,p)=1$. 这意味着 $g^n\equiv g^i(\mathrm{mod}\ Z(H))$. 由此得 $[g,n]\in\langle g\rangle$. 类似地, $[h,n]\in\langle h\rangle$. 注意到 $\langle g\rangle\bigcap\langle h\rangle\neq 1$ 且 $[g,n]\neq 1\neq[h,n]$. 则 $\langle[g,n]\rangle\bigcap\langle[h,n]\rangle\neq 1$. 与 (i) 的论证类似可得矛盾.

(iii) 由引理 14.11.1(3) 不妨设 $o(h)\leqslant o(g)$. 由 [53] 中的引理 2.1.6 知, 存在整数 u 使得 $\langle g\rangle\bigcap\langle g^uh\rangle=1$. 由引理 14.11.1(4) 推出 $[g,n,g^uh]\in\langle g\rangle\bigcap\langle g^uh\rangle$. 因而 $1=[g,n,g^uh]=[g,n,h][g,n,g^u]^h=[g,n,h]$. 这与 $[g,n,h]\neq 1$ 矛盾. 于是 $N(H/Z(H))=Z(H/Z(H))$. 从而 $N(G)=Z(G)$. □

定理 14.11.8　设 G 是非交换的奇阶亚循环 p 群, 如定理 6.1.3所设. 则

(1) $N(G)\neq Z_2(G)$.

(2) 对于 $t\geqslant u\geqslant 0, N(G)=\langle a^{p^s},b^{p^{s+u}}\rangle$; 对于 $0\leqslant t<u, N(G)=\langle a^{p^{s+u-t}},b^{-p^{s+t}}a^{p^s}\rangle$.

(3) $N(G)=Z(G)$ 当且仅当 $u=0$.

证明　由定理 6.1.3, 不妨设

$$G=\langle a,b\mid a^{p^{r+s+u}}=1,b^{p^{r+s+t}}=a^{p^{r+s}},[a,b]=a^{p^r}\rangle,$$

其中 $r\geqslant 1,u,s,t\geqslant 0$ 且 $u\leqslant r$. 进一步地, $\exp(G)=o(b)$, $Z(G)=\langle a^{p^{s+u}}\rangle\langle b^{p^{s+u}}\rangle$ 且 $G'=\langle a^{p^r}\rangle$.

(1) 令 $\overline{G}=G/Z(G)$. 则

$$\overline{G}=\langle\bar{a},\bar{b}\mid\bar{a}^{p^{s+u}}=1,\ \bar{b}^{p^{s+u}}=1,\ [\bar{a},\bar{b}]=\bar{a}^{p^r}\rangle.$$

若 $r\geqslant s+u$, 则 $\overline{G}$ 交换. 故 $Z(\overline{G})=\overline{G}$. 从而 $Z_2(G)=G$. 因为 $N(G)$ 交换, 故 $N(G)\neq Z_2(G)$. 若 $r<s+u$, 则 $Z(\overline{G})=\langle\bar{a}^{p^{s+u-r}}\rangle\langle\bar{b}^{p^{s+u-r}}\rangle$. 故 $Z_2(G)=\langle a^{p^{s+u-r}},b^{p^{s+u-r}}\rangle$. 设 $N(G)=Z_2(G)$. 注意到 $b^{b^{p^{s+u-r}}}=b$ 且 $\exp(G)=o(b)$. 则由引理 14.11.3(1) 可知, 对于所有的 $g\in G$ 有 $g^{b^{p^{s+u-r}}}=g$. 于是 $b^{p^{s+u-r}}\in Z(G)$. 这矛盾与 $Z(G)=\langle a^{p^{s+u}}\rangle\langle b^{p^{s+u}}\rangle$.

(2) 首先断言 $N(G)=N_G(\langle b\rangle)\bigcap C_G(b^{-p^t}a)$. 证明如下:

设 $g\in G$, 则 g 可写成 $g=b^ja^i$ 的形式, 其中 i 和 j 是非负整数. 设 $b^ja^i\in G$, $b^ja^i\in N(G)$. 则 $b^{b^ja^i}=b^{a^i}=b[b,a]^i\in\langle b\rangle$. 从而 $p^s|i$. 令 $i=i_1p^s$, 其中 i_1 是整数. 则 $b^{b^ja^i}=b^{1-i_1p^{r+s+t}}$. 由引理 14.11.3(1) 可得, $(b^{-p^t}a)^{b^ja^i}=(b^{-p^t}a)^{1-i_1p^{r+s+t}}$. 因为

$o(b^{-p^t}a) = p^{r+s}$, 故 $(b^{-p^t}a)^{b^ja^i} = b^{-p^t}a$. 从而 $N(G) \leqslant C_G(b^{-p^t}a)$. 显然, $N(G) \leqslant N_G(\langle b\rangle)$. 于是 $N(G) \leqslant N_G(\langle b\rangle)\bigcap C_G(b^{-p^t}a)$. 反之, 设 $b^ja^i \in N_G(\langle b\rangle)\bigcap C_G(b^{-p^t}a)$. 则 $b^{b^ja^i} = b^{a^i} = b[b,a]^i \in \langle b\rangle$. 从而 $p^s|i$. 令 $i = i_1p^s$, 其中 i_1 是整数. 则 $b^{b^ja^i} = b^{1-i_1p^{r+s+t}}$. 因为

$$[b^{-p^t}a, b^ja^i] = [b^{-p^t}a, a^i][b^{-p^t}a, b^j] = [b^{-p^t}, a]^i[a, b^j] = 1,$$

故 $[a, b^j] = a^{-i_1p^{r+s+t}}$. 于是 $a^{b^ja^i} = a^{b^j} = a^{1-i_1p^{r+s+t}}$. 对 $b^la^k \in G$ 有

$$(b^la^k)^{b^ja^i} = b^{l(1-i_1p^{r+s+t})}a^{k(1-i_1p^{r+s+t})} = b^la^kb^{-li_1p^{r+s+t}}a^{-ki_1p^{r+s+t}} = (b^la^k)^{1-i_1p^{r+s+t}}.$$

于是 $b^ja^i \in N(G)$.

现在计算 $N(G)$. 设 $b^ja^i \in N_G(\langle b\rangle)\bigcap C_G(b^{-p^t}a)$. 由上述证明可得

$$b^{b^ja^i} = b^{1-i_1p^{r+s+t}}, \quad [b^{-p^t}a, b^ja^i] = [b^{-p^t}, a]^i[a, b^j] = a^{i_1p^{r+s+t}}[a, b^j] = 1,$$

其中 $i = i_1p^s$. 以下考虑两种情形: (i) $t \geqslant u \geqslant 0$, (ii) $0 \leqslant t < u$.

(i) $t \geqslant u \geqslant 0$.

因为 $[b^{-p^t}a, b^ja^i] = a^{i_1p^{r+s+t}}[a, b^j] = 1$ 和 $o(a) = p^{r+s+u}$, 故 $[a, b^j] = 1$. 这意味着 $b^j \in Z(G)$. 注意到 $Z(G) = \langle a^{p^{s+u}}, b^{p^{s+u}}\rangle$. 我们有 $p^{s+u}|j$. 故 $N(G) \leqslant \langle a^{p^s}, b^{p^{s+u}}\rangle$. 另一方面, 显而易见, $a^{p^s}, b^{p^{s+u}} \in N(G)$. 于是 $N(G) = \langle a^{p^s}, b^{p^{s+u}}\rangle$.

(ii) $0 \leqslant t < u$.

因为 $[b^{-p^t}a, b^ja^i] = a^{i_1p^{r+s+t}}a^{-1}a^{(1+p^r)^j} = 1$, 故

$$(1+p^r)^j - 1 \equiv -i_1p^{r+s+t} (\mathrm{mod}\ p^{r+s+u}).$$

于是 $(1+p^r)^j \equiv 1 (\mathrm{mod}\ p^{r+s+t})$. 从而 $p^{s+t}|j$. 令 $j = j_1p^{s+t}$, 其中 j_1 是整数. 由 $a^{i_1p^{r+s+t}}a^{-1}a^{(1+p^r)^j} = a^{i_1p^{r+s+t}}a^{j_1p^{r+s+t}} = 1$ 可得 $i_1 \equiv -j_1 (\mathrm{mod}\ p^{u-t})$. 不妨设 $j_1 = -i_1 + np^{u-t}$, 其中 n 是整数. 则

$$b^ja^i = b^{j_1p^{s+t}}a^{i_1p^s} = b^{(-i_1+np^{u-t})p^{s+t}}a^{i_1p^s}.$$

注意到 $(b^{-p^{s+t}}a^{p^s})^{i_1} = b^{-i_1p^{s+t}}[b^{-p^{s+t}}, a^{-p^s}]\binom{i_1}{2}a^{i_1p^s} = b^{-i_1p^{s+t}}a^{i_1p^s}[b^{-p^{s+t}}, a] - p^s\binom{i_1}{2}$ 且 $[b^{-p^{s+t}}, a] - p^s\binom{i_1}{2} \in \langle a^{p^{s+u-t}}\rangle$. 则

$$N(G) \leqslant \langle a^{p^{s+u-t}}, b^{-p^{s+t}}a^{p^s}, b^{p^{s+u}}\rangle = \langle a^{p^{s+u-t}}, b^{-p^{s+t}}a^{p^s}\rangle.$$

不难看到, $a^{p^{s+u-t}}, b^{-p^{s+t}}a^{p^s} \in N(G)$. 于是 $N(G) = \langle a^{p^{s+u-t}}, b^{-p^{s+t}}a^{p^s}\rangle$.

(3) 由 (2) 可知, $N(G) = Z(G)$ 当且仅当 $u = 0$. □

推论 14.11.9 设 G 是奇数阶的二元生成的 p 群. 若 $N(G)=Z_2(G)\neq Z(G)$, 则 $N(G)\leqslant\Phi(G)$.

证明 设 $N(G)\nleqslant\Phi(G)$. 选择 $a\in N(G)\backslash\Phi(G)$ 和 $b\in G\backslash\Phi(G)$ 使得 $G=\langle a,b\rangle$. 则 $G=\langle a\rangle\langle b\rangle$. 由 [89] 中的III, 定理 11.5 可知, G 亚循环. 然而, 由定理 14.11.8 可得, $N(G)\neq Z_2(G)$. 矛盾. □

定理 14.11.10 设 G 是二元生成导群循环的 p 群且 $p>2$. 则 $N(G)=Z(G)$ 当且仅当 G 同构于下列互不同构的群之一.

(1) $\langle a,b\mid a^{p^{r+s}}=1,b^{p^{r+s+t}}=1,[a,b]=a^{p^r}\rangle$, $r\geqslant 1,\ s,\ t\geqslant 0$;

(2) $\langle a,b,c\mid a^{p^n}=b^{p^m}=c^{p^r}=1,[a,b]=c,[c,a]=c^{p^s},[c,b]=c^{p^t}\rangle$, $n\geqslant m\geqslant r,t=r$ 或 $s\leqslant t<\min\{r,n-m+s\}$;

(3) $\langle a,b,c\mid a^{p^{n-u+r}}=c^{p^r},b^{p^n}=c^{p^u}=1,[a,b]=c,[c,a]=c^{p^s},[c,b]=1\rangle$, $r<u<n,r+s\geqslant u,n-u+r\geqslant u,s\leqslant u$;

(4) $\langle a,b,c\mid a^{p^{n-u+r}}=c^{p^r},b^{p^n}=c^{p^u}=1,[a,b]=c^{\sigma},[c,a]=1,[c,b]=c^{p^t}\rangle$, $r<u\leqslant n,t<u,p\nmid\sigma$, 对 σ 有

$$\begin{cases}\sigma\leqslant\min\{p^{u-r},p^{u-t}\}, & n-u+r\geqslant u,\\ \sigma\leqslant\min\{p^{t},p^{u-t}\}\text{ 且 }\sigma\equiv 1(\operatorname{mod}\ p^{u-r-t}), & n-u+r<u,\ n-u=t;\end{cases}$$

(5) $\langle a,b,c\mid a^{p^{n-u+r}}=c^{p^r},b^{p^n}=c^{p^u}=1,[a,b]=c^{\sigma},[c,a]=c^{p^s},[c,b]=c^{p^t}\rangle$, $r<u\leqslant n,\ r+s\geqslant u,t<s<\min\{u-r+t,u\}$, $p\nmid\sigma$, 对 σ 有

$$\begin{cases}\sigma\leqslant\min\{p^{u-r},p^{s-t}\}, & n-u+r\geqslant u,\\ \sigma\leqslant\min\{p^{t},p^{s-t}\}\text{ 且 }\sigma\equiv 1(\operatorname{mod}\ p^{u-r-t}), & n-u+r<u,\ n-u=t;\end{cases}$$

(6) $\langle a,b,c\mid a^{p^n}=c^{p^u}=1,b^{p^{m-u+r}}=c^{p^r},[a,b]=c^{\sigma},[c,a]=c^{p^s},[c,b]=1\rangle$, $r<u<m<n,s\leqslant u,p\nmid\sigma,\sigma\, p^{m-u+r}+p^{r+s}\equiv 0(\operatorname{mod}\ p^u)$, 对 σ 有

$$\begin{cases}\sigma\leqslant\min\{p^{u-r},p^{u-s}\}, & n-m+u-r\geqslant u-s,\\ \sigma\leqslant p^{u-r}, & n-m+u-r<u-s;\end{cases}$$

(7) $\langle a,b,c\mid a^{p^n}=c^{p^u}=1,b^{p^{m-u+r}}=c^{p^r},[a,b]=c,[c,a]=1,[c,b]=c^{p^t}\rangle$, $r<u<m<n,t<u,m-u+r\geqslant u,r+t\geqslant u$;

(8) $\langle a,b,c\mid a^{p^n}=c^{p^u}=1,b^{p^{m-u+r}}=c^{p^r},[a,b]=c^{\sigma},[c,a]=c^{p^s},[c,b]=c^{p^t}\rangle$, $r<u<m<n,r+t\geqslant u,s<t<\min\{n-m+u-r+s,u\},p\nmid\sigma,\sigma\, p^{m-u+r}+p^{r+s}\equiv 0(\operatorname{mod}\ p^u)$, $\sigma\leqslant\min\{p^{t-s},p^{u-r}\}$.

证明 由定理 10.2.2 可知, G 正则且 $|G/\mho_1(G)|\leqslant p^3$. 以下分两种情形讨论: $|G/\mho_1(G)|\leqslant p^2$ 或 $|G/\mho_1(G)|=p^3$.

(i) $|G/\mho_1(G)| \leqslant p^2$.

由 [89] 中的III, 定理 11.4 可知, G 是亚循环的. 由定理 14.11.8(3) 可得, G 是群 (1).

(ii) $|G/\mho_1(G)| = p^3$.

则 G 是定理 10.2.3 和定理 10.2.4 中的群之一, 且 $G' = \langle c\rangle$.

若 G 是定理 10.2.3 中的群, 因为 c 是 G 的唯一性基中的元, 由引理 14.11.5 可知, $N(G) = Z(G)$. 因而 G 是群 (2).

若 G 是定理 10.2.4 中的III型群, 我们只需证 $N(G) = Z(G)$ 当且仅当 $n = m$. 事实上, 若 $n = m$, 因为 $o(b) = \exp(G)$ 和 $\langle b\rangle \bigcap \langle c\rangle = 1$, 由引理 14.11.4(1) 可得, $N(G) = Z(G)$. 若 $n > m$, 我们将证明 $b^{p^{u-1}} \in N(G) \setminus Z(G)$. 从而 $N(G) \neq Z(G)$. 设 $b^{p^{u-1}} \in Z(G)$. 则 $[a, b^{p^{u-1}}] = [a, b]^{p^{u-1}} = c^{p^{u-1}} = 1$. 与 $o(c) = p^u$ 矛盾. 对 $g \in G$, 则 g 可写成 $g = a^i b^j c^k$ 的形式, 其中 i, j 和 k 是非负整数. 因为

$$a^{b^{p^{u-1}}} = a[a, b^{p^{u-1}}] = ac^{p^{u-1}} c^{p^t\binom{p^{u-1}}{2}} c^{p^{2t}\binom{p^{u-1}}{3}} \cdots = ac^{p^{u-1}} = a^{1+p^{n-1}}$$

且 $c^{b^{p^{u-1}}} = c[c, b^{p^{u-1}}] = cc^{p^{t+u-1}} = c$, 故

$$\begin{aligned}(a^i b^j c^k)^{b^{p^{u-1}}} &= a^{i(1+p^{n-1})} b^j c^k \\ &= a^i b^j c^k a^{ip^{n-1}} \qquad (\text{因为 } a^{p^{n-1}} \in Z(G)) \\ &= a^i b^j c^k (a^i b^j c^k)^{p^{n-1}} (\text{因为 } G \text{ 是 } p^{n-1} \text{ 交换的 且 } o(c) < o(b) \leqslant p^{n-1}) \\ &= (a^i b^j c^k)^{1+p^{n-1}}.\end{aligned}$$

由此可得 $b^{p^{u-1}} \in N(G)$. 若 G 是定理 10.2.4 中的 (I) 型群或 (II) 型群, 同理可证 $N(G) = Z(G)$ 当且仅当 $n = m$. 于是我们得到 G 是群 (3)—(5).

设 G 是定理 10.2.4 中的 (IV) 型群. 我们只需证 $N(G) = Z(G)$ 当且仅当 $r + \theta = u$. 若 $r + \theta = u$, 因为 $o(a) = \exp(G)$ 且 $\langle a\rangle \bigcap \langle c\rangle = 1$, 由引理 14.11.4(1) 可知, $N(G) = Z(G)$. 若 $r + \theta < u$, 我们将证明 $b^{p^{u-1}} \in N(G) \setminus Z(G)$. 从而 $N(G) \neq Z(G)$. 设 $b^{p^{u-1}} \in Z(G)$. 则 $[a, b^{p^{u-1}}] = [a, b]^{p^{u-1}} = c^{p^{u-1}} = 1$, 这与 $o(c) = p^u$ 矛盾. 对 $g \in G$, 则 g 可写成 $g = a^{i_1} b^j c^k$ 的形式, 其中 i, j 和 k 是非负整数. 因为

$$a^{b^{p^{u-1}}} = a[a, b^{p^{u-1}}] = ac^{p^{u-1}} c^{p^t\binom{p^{u-1}}{2}} c^{p^{2t}\binom{p^{u-1}}{3}} \cdots = ac^{p^{u-1}} = a^{1+i^{-1}p^{n-1}}$$

且 $c^{b^{p^{u-1}}} = c[c, b^{p^{u-1}}] = cc^{p^{t+u-1}} = c$, 故

$$\begin{aligned}(a^{i_1} b^j c^k)^{b^{p^{u-1}}} &= a^{i_1(1+i^{-1}p^{n-1})} b^j c^k \\ &= a^{i_1} b^j c^k a^{i_1 i^{-1} p^{n-1}} \qquad (\text{因为 } a^{p^{n-1}} \in Z(G)) \\ &= a^{i_1} b^j c^k (a^{i_1} b^j c^k)^{i^{-1}p^{n-1}} (\text{因为 } G \text{ 是 } p^{n-1} \text{ 交换 且 } o(c) < o(b) \leqslant p^{n-1}) \\ &= (a^{i_1} b^j c^k)^{1+i^{-1}p^{n-1}}.\end{aligned}$$

于是得 $b^{p^{u-1}} \in N(G)$. 若 G 是定理 10.2.4 中的 (V) 型群或 (VI) 型群, 同理可证 $N(G) = Z(G)$ 当且仅当 $r + \theta = u$. 于是我们得到 G 是群 (6)—(8). □

推论 14.11.11　设 G 是幂零群但不是 2 群, G' 循环. 若 G 有奇数阶 Sylow p 子群 P 使得 P 非交换, 则 $N(G) \neq Z_2(G)$.

证明略去. □

例 14.11.12　设 $G = \langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, [a,b] = a^{-2}\rangle$, $n \geqslant 4$. 不难看出, G 是极大类 2 群, 且 G' 循环. 进一步地, $Z_2(G) = G_{n-2} = \langle a^{2^{n-3}}\rangle$. $a^{2^{n-3}} \in N_G(\langle a^i\rangle)$. 于是 $N(G) = Z_2(G)$.

定理 14.11.13　设 G 是有限 p 群, G' 循环且 $p > 2$. 令 $\exp(G) = p^n$ 和 $\exp(N(G)/Z(G)) = p^k$, 其中 n 和 k 是正整数. 则

(1) $n \geqslant 2k$;

(2) $G = \langle g, C_G(N(G))\rangle$, 其中 $o(g) = p^n$, $g^{p^k} \in C_G(N(G))$, $C_G(N(G)) < G$ 且 $\exp(C_G(N(G))) = p^{n-k}$;

(3) $n = 2k$ 当且仅当 $G = AB$, 其中 $A \trianglelefteq G$ 和 $B \trianglelefteq G$ 且满足

(i) $A = \langle g\rangle$ 且 $o(g) = p^{2k}$, $g^{p^k} \in B$,

(ii) $c(B) \leqslant 2$, $\exp(B) = p^k$ 且 $B' \leqslant \langle g^{p^k}\rangle$. 存在 $a \in Z(B)$ 使得 $[g, B] = \langle [g, a]\rangle = \langle g^{p^k}\rangle$;

(4) $C_G(N(G)) = N(G)$ 当且仅当 $G = C \rtimes D$, 其中 $C \trianglelefteq G$, C 和 D 满足以下性质

(i) $C = \langle g\rangle$ 且 $o(g) = \exp(G)$,

(ii) D 是交换 p 群, $\exp(D) \leqslant p^{n-k}$ 且 $[g, D] = \langle g^{p^{n-k}}\rangle$.

证明　(1) 因为 G' 循环, 故 G 是正则 p 群. 由引理 14.11.3(2) 得 $N(G)/Z(G)$ 循环. 令 $N(G)/Z(G) = \langle aZ(G)\rangle$. 则 $N(G) = \langle a, Z(G)\rangle$ 且 $a^{p^k} \in Z(G)$. 选择 $g \in G$ 使得 $o(g) = p^n$. 再令 $g^a = g^i$, 其中 i 是正整数且 $p \nmid i$. 因为 $N(G) \neq Z(G)$, 由引理 14.11.3(1) 得, $i \not\equiv 1 (\mathrm{mod}\ p^n)$. 注意到 $a^{p^k} \in Z(G)$. 则 $i^{p^k} \equiv 1 (\mathrm{mod}\ p^n)$.

令 $\overline{G} = G/Z(G)$. 由定理 14.11.7(1) 易得 $N(\overline{G}) = Z(\overline{G})$. 故对 $\bar{g} \in \overline{G}$ 有 $\bar{g}^{\bar{a}} = \overline{g^a} = \overline{g^i} = \bar{g}$. 从而 $g^{i-1} \in Z(G)$. 因为 $(g^{i-1})^a = (g^a)^{i-1} = g^{i(i-1)} = g^{i-1}$, 故 $i(i-1) \equiv i - 1 (\mathrm{mod}\ p^n)$. 于是我们有下列方程:

$$\begin{cases} i \not\equiv 1 (\mathrm{mod}\ p^n), \\ i^{p^k} \equiv 1 (\mathrm{mod}\ p^n), \\ i(i-1) \equiv i - 1 (\mathrm{mod}\ p^n). \end{cases}$$

由此可得 $i = 1 + jp^{n-k}$, 其中 $p \nmid j$ 且 $n \geqslant 2k$.

(2) 由 (1) 的证明可得, $g^a = g^{1+jp^{n-k}}$. 从而对 $h \in G$, 由引理 14.11.3(1) 可得, $h^a = h^{1+jp^{n-k}}$. 于是 $|[G, a]| = \exp([G, a]) = o([g, a]) = p^k$.

考虑同态 $\varphi : G \to [G,a]$. 则 $G/C_G(a) \cong [G,a] \cong C_{p^k}$. 因为 $C_G(a) = C_G(N(G))$, 故 $G/C_G(N(G)) \cong C_{p^k}$. 注意到 $g^a = g^{1+jp^{n-k}}$ 且 $o(g) = p^n$. 则 $g^{p^k} \in C_G(N(G))$. 从而 $o(gC_G(N(G))) = p^k$. 于是 $G/C_G(N(G)) = \langle gC_G(N(G))\rangle$. 由此推出 $G = \langle g, C_G(N(G))\rangle$. 显然, $C_G(N(G)) < G$.

因为 $h^a = h^{1+jp^{n-k}}$, 故对 $b \in C_G(a)$ 有 $o(b) \leqslant p^{n-k}$. 另一方面, $g^{p^k} \in C_G(a)$ 且 $o(g^{p^k}) = p^{n-k}$. 于是 $\exp(C_G(a)) = \exp(C_G(N(G))) = p^{n-k}$.

(3) 由 $G' \leqslant C_G(N(G))$ 可得 $|G'| \leqslant p^{n-k} = p^k$. 又由 (1) 得 $o([g,a]) = p^k$. 故 $G' = \langle [g,a]\rangle = \langle g^{p^k}\rangle$. 从而 $\langle g\rangle \trianglelefteq G$. 令 $A = \langle g\rangle$ 与 $B = C_G(N(G))$. 由 (2) 得 $G = AB$ 且 $g^{p^k} \in B$. 因为 $a \in N(G)$, 故 $a \in Z(B)$. 由于 $[g,B] = \langle [g,a]\rangle = \langle g^{p^k}\rangle$, 有 $g^{p^k} \in Z(G)$. 从而 $c(B) \leqslant c(G) \leqslant 2$. 显然, $\exp(B) = p^k$ 且 $B' \leqslant \langle g^{p^k}\rangle$.

反之易证 $G' = \langle g^{p^k}\rangle \leqslant Z(G)$. 从而 G 是 p^k 交换的. 因为 $\langle [g,a]\rangle = \langle g^{p^k}\rangle$ 且 $a \in Z(B)$, 故 $a \in N(G) \setminus Z(G)$. 下证 $\exp(G) = 2\exp(N(G)/Z(G))$. 设 $n = g^s b$ $(b \in B)$ 是 G 的元素, $g^s b \in N(G)$. 则 $n^{p^k} = (g^s)^{p^k} \in Z(G)$. 这推出 $\exp(N(G)/Z(G)) \leqslant p^k$. 注意到 $a \in N(G)$ 且 $o(aZ(G)) = p^k$. 则 $\exp(N(G)/Z(G)) = p^k$. 显然, $\exp(G) = p^{2k}$.

(4) 由 (2) 得 $G = \langle g, C_G(N(G))\rangle = \langle g\rangle N(G)$, 其中 $o(g) = p^n$, $g^{p^k} \in N(G)$ 且 $\exp(N(G)) = p^{n-k}$. 因为 $N(G)$ 是交换的, 故存在群 D 使得 $N(G) = \langle g^{p^k}\rangle \times D$. 这推出 $G = C \rtimes D$, 其中 $C = \langle g\rangle$. 由 (2) 的证明可得, $G' = \langle g^{p^{n-k}}\rangle$. 于是 $[g,D] = G' = \langle g^{p^{n-k}}\rangle$.

反之易证, $c(G) = 2$ 且 $G' = \langle g^{p^{n-k}}\rangle$. 选择 $a \in D$ 使得 $[g,a] = g^{p^{n-k}}$. 对 $h \in G$, h 可写成 $h = g^i d$ $(d \in D)$ 的形式, 其中 i 是非负整数. 设 $g^i d \in N(G)$. 则

$$a^{g^i d} = a[a,g]^i = ag^{-ip^{n-k}} \in \langle a\rangle.$$

因为 $\langle g\rangle \bigcap D = 1$, 故 $p^k | i$. 从而 $N(G) \leqslant \langle g^{p^k}\rangle \times D$. 对 $d_1 \in D$, $g_1 \in G$, 不妨设 $g_1 = g^j d_2$ $(d_2 \in D)$. 则

$$g_1^{d_1} = (g^j d_2)^{d_1} = g^j [g,d_1]^j d_2 = g^j g^{tjp^{n-k}} d_2 = g^j d_2 g^{tjp^{n-k}} = (g^j d_2)^{1+tp^{n-k}} = g_1^{1+tp^{n-k}},$$

其中 t 是整数. 于是 $D \leqslant N(G)$. 注意到 $g^{p^k} \in N(G)$. 则 $N(G) = \langle g^{p^k}\rangle \times D$.

设 $w = g^l d_3 \in C_G(N(G))$, 其中 $d_3 \in D$ 且 l 是整数. 则 $a^w = a^{g^l d_3} = a[a,g]^l = a$. 于是 $p^k | l$. 从而 $w \in N(G)$. 这推出 $C_G(N(G)) = N(G)$. □

下面列出文献 [75] 获得的其他结果, 证明略去.

定理 14.11.14 设 G 是奇数阶群. 则对正整数 i, $N(G/Z_i(G)) = \zeta(G/Z_i(G))$ 当且仅当 $[G', N(G:Z_i(G))] \leqslant Z_{i-1}(G)$, 其中 $Z_i(G)$ 是 G 的上中下群列的第 i 项.

推论 14.11.15 设 G 是奇阶幂零群, $w(G)$=$Z(G)$. 则对每个正整数 i, $w_i(G) = Z_i(G)$ 当且仅当 $[G', w(G:Z_i(G))] \leqslant Z_{i-1}(G)$.

推论 14.11.16　设 G 是奇阶亚交换群. 若 $C_G(G') = N(G : Z(G))$, 则

(1) 对每个正整数 i, $N(G/Z_i(G)) = Z(G/Z_i(G))$;

(2) $c(G) \leqslant 3$;

(3) 若 G 是 p 群, G' 循环. 则 $c(G) \leqslant 2$.

推论 14.11.17　设 G 是幂零群, G' 循环. 若 $w_i(G) \subseteq Z_r(G)$, 其中 $i \geqslant 1$, $r \geqslant 1$, 则 $w_{i+1}(G) \subseteq Z_{r+1}(G)$. 特别地,

(i) $w(G) = Z(G)$ 可推出 $w_j(G) = Z_j(G)$, $j \geqslant 1$;

(ii) $w(G) = \zeta_2(G)$ 可推出 $w_j(G) = Z_{j+1}(G)$, $j \geqslant 1$.

14.12　极大类 p 群的 Wielandt 子群

张小红等在文献 [282] 研究了极大类 p 群的 Wielandt 列和上中心群列之间的关系. 证明了极大类 p 群的任意非平凡商群都满足 Wielandt 子群和中心是一致的. 给出正则的极大类 p 群的 Wielandt 子群和上中心群列第二项一致的充要条件. 本节介绍他们的结果. 以下总假设极大类 p 群是非交换的.

引理 14.12.1　设 G 是群, $G' \bigcap Z_2(G)$ 循环. 则 $N(G/Z(G)) = Z(G/Z(G))$.

证明　设 $N(G/Z(G)) \neq Z(G/Z(G))$. 则存在 $n \in N(G : Z(G))$ 和 g, $h \in G$ 使得 $[g, n, h] \neq 1$. 注意到 $[g, n], [h, n] \in G' \bigcap Z_2(G)$. 则 $[g, n] = [h, n]^i$ 或 $[h, n] = [g, n]^j$. 若 $[g, n] = [h, n]^i$, 由引理 14.11.1(2) 得, $[g, n, h] = [[h, n]^i, h] = 1$. 同样的论证可得, 当 $[h, n] = [g, n]^j$ 时, $[h, n, g] = 1$. 于是 $[g, n, h] = 1$. 矛盾. □

定理 14.12.2　设 G 是 p^n 阶的极大类 p 群. 则

(1) 若 $w_i(G) \subseteq Z_r(G)$, 则 $w_{i+1}(G) \subseteq Z_{r+1}(G)$, 其中 $i \geqslant 1$, $r \geqslant 1$;

(2) 对所有整数 i, $w_i(G) = Z_i(G)$, 或 $w_i(G) = Z_{i+1}(G)$ 除非 $G \cong \mathrm{M}_p(2,1)$, 其中 $p > 2$;

(3) 若 $1 < K \trianglelefteq G$, 则 $w(G/K) = Z(G/K)$.

证明　(1) 由定理 1.11.8 可得, $|Z(G)| = p$, 进一步地, 若 $p > 2$ 且 $n > 3$, 则 $Z_2(G) \cong \mathrm{C}_p \times \mathrm{C}_p$. 断言对任意正整数 i 有 $w(G/Z_i(G)) = Z(G/Z_i(G))$. 分 $p > 2$ 和 $p = 2$ 讨论.

(i) $p > 2$.

对于 $n \leqslant 3$, 显然 $w(G/Z_i(G)) = Z(G/Z_i(G))$. 设 $n \geqslant 4$. 先考虑 $i = 1$ 的情况. 令 $\overline{G} = G/Z(G)$ 并设 $w(\overline{G}) \neq Z(\overline{G})$. 则存在 $n \in w(G : Z(G))$ 和 g, $h \in G$ 使得 $[g, n, h] \neq 1$. 因为 $[g, n, h] \in Z(G)$ 和 $|Z(G)| = p$, 故 $Z(G) = \langle [g, n, h] \rangle$. 注意到 $[g, n] \in Z_2(G)$, $[h, n] \in Z_2(G)$ 和 $Z_2(G) \cong \mathrm{C}_p \times \mathrm{C}_p$, 则 $Z_2(G) = \langle [g, n] \rangle \times \langle [h, n] \rangle$. 故 $[h^j, [g, n]] = ([h, [g, n]])^j = [g, n][h, n]^i$, 其中 $p \nmid ij$. 这意味着 $h^{-j}[g, n]^{-1}h^j = [h, n]^i$. 从而 $[g, n]^{-1} = [h, n]^i$. 矛盾.

对于 $i \geqslant 2$, 若 $|G/Z_i(G)| \leqslant p^2$, 则 $w(G/Z_i(G)) = Z(G/Z_i(G))$. 设 $|G/Z_i(G)| \geqslant p^3$. 则 $|G/Z_{i-1}(G)| \geqslant p^4$. 由定理 1.11.8 可得, $G/Z_{i-1}(G)$ 是极大类 p 群. 由对 $i = 1$ 的证明可知,

$$w(G/Z_{i-1}(G)/Z(G/Z_{i-1}(G))) = Z(G/Z_{i-1}(G)/Z(G/Z_{i-1}(G))).$$

因为

$$G/Z_{i-1}(G)/Z(G/Z_{i-1}(G)) = G/Z_{i-1}(G)/Z_i(G)/Z_{i-1}(G) \cong G/Z_i(G),$$

故 $w(G/Z_i(G)) = Z(G/Z_i(G))$.

(ii) $p = 2$.

若 G 是极大类 2 群, 则 G 是亚循环 p 群. 由引理 14.12.1 可得, $w(G/Z(G)) = Z(G/Z(G))$. 对于 $i \geqslant 2$, 因为 $(G/Z_i(G))'$ 循环, 再由引理 14.12.1 可得

$$w(G/Z_{i-1}(G)/Z(G/Z_{i-1}(G))) = Z(G/Z_{i-1}(G)/Z(G/Z_{i-1}(G))).$$

注意到

$$G/Z_{i-1}(G)/Z(G/Z_{i-1}(G)) = G/Z_{i-1}(G)/Z_i(G)/Z_{i-1}(G) \cong G/Z_i(G).$$

我们有 $w(G/Z_i(G)) = Z(G/Z_i(G))$.

令 $w \in w_{i+1}(G)$. 则对 $g \in G$, 存在 k 使得 $g^w \equiv g^k (\mathrm{mod}\ w_i(G))$. 因而 $g^{-k}g^w \in w_i(G) \leqslant Z_r(G)$. 令 $\overline{G} = G/Z_r(G)$. 因为 $g^{-k}g^w \in Z_r(G)$, 故 $\bar{g}^{\bar{w}} = \bar{g}^k$. 于是 $w_{i+1}(G)Z_r(G)/Z_r(G) \leqslant w(G/Z_r(G))$. 注意到

$$w(G/Z_r(G)) = Z(G/Z_r(G)) = Z_{r+1}(G)/Z_r(G).$$

我们有 $w_{i+1}(G) \subseteq Z_{r+1}(G)$.

(2) 首先断言 $w(G) = Z(G)$, 或 $w(G) = Z_2(G)$ 除非 $G \cong \mathrm{M}_p(2,1)$, 其中 $p > 2$.

若 $n > 3$, 由定理 1.11.8 可得, $|Z(G)| = p$ 且 $|Z_2(G)| = p^2$. 因为 $Z(G) \leqslant w(G) \leqslant Z_2(G)$, 故 $w(G) = Z(G)$ 或 $w(G) = Z_2(G)$.

设 $n = 3$. 由定理 1.7.10 知, G 同构于 Q_8, $\mathrm{M}_p(1,1,1)$ 或 $\mathrm{M}_p(2,1)$ 之一.

若 $G \cong \mathrm{Q}_8$, 则 $w(G) = Z_2(G)$. 若

$$G \cong \mathrm{M}_p(1,1,1) = \langle a, b, c \mid a^p = b^p = c^p = 1, [a,b] = c \rangle,$$

则对任意的 $a^ib^jc^k \in w(G)$ 有 $a^{a^ib^jc^k} \in \langle a \rangle$. 故 $p \mid j$. 同理可证 $p \mid i$. 由此可得 $w(G) = Z(G)$. 设

$$G \cong \mathrm{M}_p(2,1) = \langle a, b \mid a^{p^2} = b^p = 1,\ [a,b] = a^p \rangle,$$

其中 $p > 2$. 下证 $w(G) = \langle b, a^p\rangle$. 因为

$$(b^j a^i)^b = b^j a^i [a,b]^i = b^j a^i a^{ip} = (b^j a^i)^{1+p}, \quad a^p \in Z(G),$$

故 $\langle b, a^p\rangle \leqslant w(G)$. 注意到 $\langle b, a^p\rangle \lessdot G$. 我们有 $w(G) = \langle b, a^p\rangle$.

若 $w_i(G) = Z_r(G)$, 则

$$w_{i+1}(G)/w_i(G) = w(G/w_i(G)) = w(G/Z_r(G)) = Z(G/Z_r(G)) = Z_{r+1}(G)/Z_r(G).$$

由此可得 $w_{i+1}(G) = Z_{r+1}(G)$. 因为 $w(G) = Z(G)$, 或 $w(G) = Z_2(G)$ 除非 $G \cong \mathrm{M}_p(2,1)$, 其中 $p > 2$, 归纳可得, $w_i(G) = Z_i(G)$ 或 $w_i(G) = Z_{i+1}(G)$ 除非 $G \cong \mathrm{M}_p(2,1)$.

(3) 若 $|K| \geqslant p^{n-1}$, 则 $w(G/K) = Z(G/K)$. 设 $|K| = p^{n-i}(2 \leqslant i \leqslant n-1)$. 因为 G_i 是 G 的唯一的 p^{n-i} 阶正规子群, 故 $K = G_i$. 注意到 $G_i = Z_{n-i}(G)$. 则 $K = Z_{n-i}(G)$. 由 (1) 的证明可得, $w(G/Z_{n-i}(G)) = Z(G/Z_{n-i}(G))$. 因而 $w(G/K) = Z(G/K)$. □

注 14.12.3 定理 14.12.2 表明存在一类 p 群, 这类群中的每个群 G 以及 G 的每个非平凡正规子群 K 均有 $w(G/K) = Z(G/K)$. 然而, 后面的例 14.12.5 和例 14.12.6 说明, 一般情形下, 定理 14.12.2 不一定成立.

推论 14.12.4 设 G 是 p^n 阶极大类 p 群, $w_r(G) \subseteq Z_i(G)$, 其中 $n \leqslant 5, r \geqslant 1$ 且 $i \geqslant 1$. 则 $w_{r+1}(G) \subseteq Z_{i+1}(G)$.

证明 若 $G/Z(G) \cong \mathrm{Q}_8$, 不妨设

$$G/Z(G) = \langle \bar{a}, \bar{b} \mid \bar{a}^4 = 1, \bar{a}^2 = \bar{b}^2, [\bar{a}, \bar{b}] = \bar{a}^2\rangle.$$

则 $a^2 \equiv b^2 (\mathrm{mod}\ Z(G))$. 从而 $a^2 \in Z(G)$. 矛盾. 设 $G/Z(G) \cong \mathrm{M}_p(2,1)$. 不妨设

$$G/Z(G) = \langle \bar{a}, \bar{b} \mid \bar{a}^{p^2} = 1, \bar{b}^p = 1, [\bar{a}, \bar{b}] = \bar{a}^p\rangle.$$

则 $G' = \langle [a,b]\rangle$. 由引理 14.12.1 可知, $w(G/Z(G)) = Z(G/Z(G))$. 然而, 定理 14.12.2(2) 告诉我们, $w(G/Z(G)) \neq Z(G/Z(G))$. 矛盾. 故 $G/Z(G)$ 交换或当 $n \leqslant 4$ 时同构于 $\mathrm{M}_p(1,1,1)$. 又由定理 14.12.2(2) 得, 当 $n \leqslant 4$ 时, $w(G/Z(G)) = Z(G/Z(G))$.

设 $n = 5$. 若 $|Z(G)| \geqslant p^2$, 由上述论证可知 $w(G/Z(G)) = Z(G/Z(G))$. 若 $|Z(G)| = p$, 只需讨论三种情形: (i) $c(G) \leqslant 2$; (ii) $c(G) = 4$; (iii) $c(G) = 3$.

(i) 若 $c(G) \leqslant 2$, 结论显然成立.

(ii) 若 $c(G) = 4$, 由定理 14.12.2(1) 的证明也可得结论成立.

(iii) 设 $c(G) = 3$. 则 $|G'| = p^2$ 或 $|G'| = p^3$. 若 $G' \cong \mathrm{C}_p \times \mathrm{C}_p$, 与定理 14.12.2(1) 的相同的论证可得, $w(G/Z(G)) = Z(G/Z(G))$. 若 $G' \cong \mathrm{C}_{p^2}$, 由引理 14.12.1 可知,

$w(G/Z(G)) = Z(G/Z(G))$. 不妨设 $|G'| = p^3$. 则 $|G/Z(G)| = p^4$, $c(G/Z(G)) = 2$ 且 $d(G/Z(G)) = 2$. 由此可得 $Z(G/Z(G)) = (G/Z(G))' = \Phi(G/Z(G))$. 从而 $G/Z(G)$ 内交换. 这与 $|(G/Z(G))'| = p^2$ 矛盾.

对于 $i \geqslant 2$, 因为 $|G/Z_{i-1}(G)| \leqslant p^4$ 且

$$G/Z_{i-1}(G)/Z(G/Z_{i-1}(G)) = G/Z_{i-1}(G)/Z_i(G)/Z_{i-1}(G) \cong G/Z_i(G),$$

故 $w(G/Z_i(G)) = Z(G/Z_i(G))$. 与定理 14.12.2(1) 相同的论证可得结论. □

例 14.12.5 设 $G = \langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [b, a] = c, [c, a] = a^p, [c, b] = b^p\rangle$, 其中 $p \geqslant 5$. 显而易见, $Z(G) = \langle a^p,\ b^p\rangle$. 故 $\langle b^p\rangle \trianglelefteq G$. 令

$$\overline{G} = G/\langle b^p\rangle = \langle \bar{a}, \bar{b}, \bar{c} \mid \bar{a}^{p^2} = \bar{b}^p = \bar{c}^p = \bar{1},\ [\bar{b}, \bar{a}] = \bar{c},\ [\bar{c}, \bar{a}] = \bar{a}^p\rangle.$$

对任意的 $\bar{a}^i\bar{b}^j\bar{c}^k \in \overline{G}$, 有

$$(\bar{a}^i\bar{b}^j\bar{c}^k)^{\bar{c}} = (\bar{a}^i)^{1-p}\bar{b}^j\bar{c}^k = (\bar{a}^i\bar{b}^j\bar{c}^k)^{1-p}.$$

故 $\bar{c} \in w(\overline{G}) \setminus Z(\overline{G})$. 从而 $w(\overline{G}) > Z(\overline{G})$. 于是存在非交换 p 群满足 $w(G/K) > Z(G/K)$, 其中 $K \trianglelefteq G$ 且 $1 < K < G$.

例 14.12.6 设 $G = \langle a, b, c, d \mid a^{3^n} = b^{3^n} = d^{3^n} = c^3 = 1,\ [a, b] = d,\ [b, c] = b^{-3^{n-1}},\ [c, a] = a^{3^{n-1}}d^{-3^{n-1}},\ [d, c] = d^{3^{n-1}},\ [d, a] = [d, b] = 1\rangle$, 其中 $n \geqslant 2$. 显而易见, $Z(G) = \langle d^3\rangle$. 故 $\overline{G} = G/Z(G) = \langle \bar{a}, \bar{b}, \bar{c}, \bar{d} \mid \bar{a}^{3^n} = \bar{b}^{3^n} = \bar{c}^3 = \bar{d}^3 = \bar{1},\ [\bar{a}, \bar{b}] = \bar{d},\ [\bar{b}, \bar{c}] = \bar{b}^{-3^{n-1}},\ [\bar{c}, \bar{a}] = \bar{a}^{3^{n-1}},\ [\bar{d}, \bar{c}] = [\bar{d}, \bar{a}] = [\bar{d}, \bar{b}] = \bar{1}\rangle$. 不难看出, $c(\overline{G}) = 2$. 可证 $w(G) = Z(G)$ 且 $w_2(G) > Z_2(G)$.

定理 14.12.7 设 G 是阶为 2^n 的极大类 2 群. 则

(1) 若 $G \cong \mathrm{D}_{2^n}$ 或 SD_{2^n}, 则 $w(G) = Z(G)$;

(2) 若 $G \cong \mathrm{Q}_{2^n}$, 则 $w(G) = Z_2(G)$.

证明留给读者. □

引理 14.12.8 设 G 是正则 p 群, $w \in w(G)$. 若 $h \in G$ 满足 $o(h) = \exp(G)$ 且 $h^w = h^i$, 则对任意 $g \in G$ 有 $g^n = g^i$, 其中 i 是正整数.

证明 因为 $N(G)$ 的元在 G 上诱导一个幂自同构, 故对所有的 $g \in G$, 存在整数 m 使得 $g^w = g^m$. 若 $o(h) = \exp(G)$ 且 $h^n = h^i$, 则 $i \equiv m(\mathrm{mod}\ \exp(G))$. 于是 $g^w = g^i$. □

定理 14.12.9 设 $G = \langle g_1, g_2, \cdots, g_t\rangle$ 是正则 p 群, 其中 $o(g_i) \leqslant o(g_1) = p^m$, $\exp(Z(G)) = p^k$, $2 \leqslant i \leqslant t$. 则

(1) 若 $\exp(G) = \exp(Z(G))$, 则 $w(G) = Z(G)$.

(2) 若 $\exp(G) > \exp(Z(G))$ 且 $o(g_i) \leqslant p^{m-k}$, 则 $w(G) = Z_2(G)$ 当且仅当 $Z_2(G) \leqslant N_G(\langle g_1\rangle) \bigcap C_G(g_2) \bigcap \cdots \bigcap C_G(g_t)$.

(3) 若 G 是 p^n 阶的极大类 p 群, 则

(i) $\exp(G) \leqslant p^2$;

(ii) 若 $\exp(G) = p$, 则 $w(G) = Z(G)$;

(iii) 若 $\exp(G) = p^2$, 不妨设 $o(g_1) > o(g_2)$, 则 $w(G) = Z_2(G)$ 当且仅当 $Z_2(G) \leqslant N_G(\langle g_1\rangle)\bigcap C_G(g_2)$.

证明 (1) 选择 $g \in Z(G)$ 使得 $o(g) = \exp(G)$. 则对任意的 $w \in w(G)$ 有 $g^w = g$. 由引理 14.12.8 可得 $w(G) = Z(G)$.

(2) 令 $g_1^a = g_1^j$, 其中 $a \in Z_2(G)$ 且 j 是整数. 因为 $[g_1, a] \in Z(G)$ 且 $\exp(Z(G)) = p^k$, 故 $p^{m-k} \mid (j-1)$. 故不妨设 $j = 1 + sp^{m-k}$. 由引理 14.12.8 可得, $g_i^a = g_i$. 由此可得

$$Z_2(G) \leqslant N_G(\langle g_1\rangle)\bigcap C_G(g_2)\bigcap\cdots\bigcap C_G(g_t).$$

反之, 由以上的证明, 对 $a \in Z_2(G)$, 不妨设 $g_1^a = g_1^{1+sp^{m-k}}$. 显然, $\exp(G') \leqslant p^{m-k}$. 从而 G 是 p^{m-k} 交换的. 对于 $g_1^{i_1}g_2^{i_2}\cdots g_t^{i_t}c \in G$ 且 $a \in Z_2(G)$, 其中 $c \in G'$, 有

$$\begin{aligned}(g_1^{i_1}g_2^{i_2}\cdots g_t^{i_t}c)^a &= (g_1^{i_1})^{1+sp^{m-k}}g_2^{i_2}\cdots g_t^{i_t}c = g_1^{i_1}g_2^{i_2}\cdots g_t^{i_t}cg_1^{i_1sp^{m-k}}\\ &= (g_1^{i_1}g_2^{i_2}\cdots g_t^{i_t}c)^{1+sp^{m-k}}.\end{aligned}$$

于是 $w(G) = Z_2(G)$.

(3) 因为 G 是正则的极大类 p 群, 不妨设

$$G = \langle g_1, g_2\rangle,\ o(g_1) \geqslant o(g_2) \quad 且 \quad \langle g_1\rangle\bigcap\langle g_2\rangle = 1.$$

(i) 由 [89] 中的III, 定理 14.21 可知, $|G| \leqslant p^p$. 由 [89] 中的III, 定理 14.14 推出 $\exp(G') = p$. 故 $[g_1^p, g_2] = [g_1, g_2]^p = 1$. 因而 $g_1^p \in Z(G)$. 因为 $|Z(G)| = p$, $o(g_1) \leqslant p^2$. 同理可证 $o(g_2) \leqslant p^2$. 于是 $\exp(G) \leqslant p^2$.

(ii) 由 (1) 即得结论.

(iii) 设 $o(g_1) = o(g_2) = p^2$. 由 (i) 的证明可得, $g_1^p, g_2^p \in Z(G)$. 注意到 $|Z(G)| = p$. 则 $\langle g_1\rangle\bigcap\langle g_2\rangle \neq 1$. 矛盾. 于是 $o(g_1) = p^2$ 且 $o(g_2) = p$. 由 (2) 即得结论. □

定理 14.12.9 一般不成立. 例 14.12.10 和例 14.12.11 表明定理 14.12.9 中正则这个条件是必要的. 例 14.12.12 表明 $o(g_i) \leqslant p^{m-k}$ 这个条件也是必要的.

例 14.12.10 设 $G = \langle a, b \mid a^9 = b^3 = c^3 = 1, [a, b] = c, [c, a] = a^3, [c, b] = 1\rangle$. 显而易见, G 是 3^4 阶极大类 p 群. 由定理 1.11.8(5)可知, $Z_2(G) = G_2 = \langle c, a^3\rangle$. 因为 $(a^2b^{-1})^c = a^5b^{-1} \notin \langle a^2b^{-1}\rangle$, 故 $c \notin w(G)$. 由定理 14.12.2(2)得 $w(G) = Z(G)$. 然而, $Z_2(G) \leqslant N_G(\langle a\rangle)\bigcap C_G(b)$.

例 14.12.11 设 $G \cong Q_{2^n} = \langle a, b \mid a^{2^{n-1}} = 1,\ b^2 = a^{2^{n-2}}, [a, b] = a^{-2}\rangle$, 其中 $n \geqslant 4$. 显而易见, G 是 2^n 阶极大类 2 群. 由定理 14.12.7得, $w(G) = Z_2(G) = \langle a^{2^{n-3}}\rangle$. 然而, $a^{2^{n-3}} \notin C_G(b)$.

例 14.12.12 设 $G=\langle a,b \mid a^{p^3}=1, b^{p^2}=a^{p^2}, [a,b]=a^p\rangle$, 其中 $p\geqslant 5$. 显然, G 正则. 计算可知, $Z(G)=\langle a^{p^2}\rangle$ 且 $Z_2(G)=\langle a^p\rangle$. 因为 $b^{a^p}=b^{1-p^2}$, 故 $Z_2(G)\leqslant N_G(\langle b\rangle)\bigcap C_G(a)$. 然而, $(ba^{-1})^{a^p}=b^{1-p^2}a^{-1}\notin\langle ba^{-1}\rangle$. 故 $w(G)\neq Z_2(G)$.

下面的例子表明, 满足定理 14.12.9 的极大类正则 p 群是存在的.

例 14.12.13 设 $G=\langle a,b,c,d,e \mid a^p=b^p=c^p=d^p=e^p=1, [b,a]=c, [c,a]=d, [c,b]=[d,a]=e, [c,d]=[d,b]=[e,a]=[e,b]=[e,c]=[e,d]=1\rangle$, 其中 $p\geqslant 5$. 显然, $|G|=p^5$ 且 $c(G)=4$. 故 G 是正则的极大类 p 群. 注意到 $\exp(G)=p$. 由定理 14.12.9(3)可知, $w(G)=Z(G)$.

例 14.12.14 设 $G=\langle a,b,c,d \mid a^{p^2}=b^p=c^p=d^p=1, [b,a]=c, [c,a]=d, [c,b]=a^p, [d,a]=a^p, [d,b]=1\rangle$, 其中 $p\geqslant 5$ 且 $p\equiv 3(\mathrm{mod}\ 4)$. 显然, $|G|=p^5$, $c(G)=4$ 且 $\exp(G)=p^2$. 故 G 是正则的极大类 p 群. 从而 $Z_2(G)=G_3=\langle d,a^p\rangle$. 不难看出, $Z_2(G)\leqslant N_G(\langle a\rangle)\bigcap C_G(b)$. 由定理 14.12.9(3)可知, $w(G)=Z_2(G)$.

例 14.12.15 设 $G=\langle a,b,c,d \mid a^{p^2}=b^p=c^p=d^p=1, [b,a]=c, [c,a]=a^p, [c,b]=d, [d,a]=1, [d,b]=a^p\rangle$, 其中 $p\geqslant 5$ 且 $p\equiv 2(\mathrm{mod}\ 3)$. 显然, $|G|=p^5$, $c(G)=4$ 且 $\exp(G)=p^2$. 故 G 是正则的极大类 p 群. 从而 $Z_2(G)=G_3=\langle d,a^p\rangle$. 因为 $d\notin C_G(b)$, 由定理 14.12.9(3)可知, $w(G)=Z(G)$.

我们知道, 若 G 是奇阶极大类 p 群, 则 $w(G)$ 初等交换. 对于幂自同构群, 即 G 的幂自同构构成的群, 记为 $\mathrm{PAut}(G)$. 进一步可证如下定理.

定理 14.12.16 设 G 是非交换 p 群.

(1) 若 $Z(G)\bigcap\mho_1(G)$ 初等交换, 则

(i) 对 $\alpha\in\mathrm{PAut}(G)$ 且 $g\in G$ 有 $g^\alpha=g^{1+kp^{n-1}}$, 其中 $o(g)=p^n$, k 是整数满足 $0\leqslant k\leqslant p-1$;

(ii) $\mathrm{PAut}(G)$ 是初等交换 p 群.

(2) 若 G 是极大类的, 则 $\mathrm{PAut}(G)$ 是初等交换 p 群.

(3) 若 $Z(G)\bigcap\mho_1(G)\bigcap G'$ 初等交换, 则 $w(G)/Z(G)$ 初等交换.

证明 (1)(i) 令 $g^\alpha=g^i$, 其中 i 是整数, 满足 $(i,p)=1$ 且 $1\leqslant i\leqslant p^n-1$. 由 [88] 中的引理 5 可知, $i\equiv 1(\mathrm{mod}\ p)$. 因为每个幂自同构是中心的, $g^{i-1}\in Z(G)\bigcap\mho_1(G)$. 注意到 $\exp\ (Z(G)\bigcap\mho_1(G))=p$. 则 $o(g^{i-1})\leqslant p$. 从而 $p^{n-1}|(i-1)$. 不妨设 $i=1+kp^{n-1}$, 其中 k 是整数且 $0\leqslant k\leqslant p-1$. 于是 $g^\alpha=g^{1+kp^{n-1}}$.

(ii) 再由 [88] 中的引理 5 知, PAut(G) 是初等交换的. 不妨设

$$\mathrm{PAut}(G)=\langle\alpha_1\rangle\times\langle\alpha_2\rangle\times\cdots\times\langle\alpha_m\rangle.$$

由 (i) 得 $g^{\alpha_j}=g^{1+kp^{n-1}}$. 故 $g^{(\alpha_j)^p}=g^{(1+kp^{n-1})^p}=g$. 由此可得 $o(\alpha_j)\leqslant p$.

(2) 因为 G 是极大类的, 故 $|Z(G)|=p$. 由 (1) 得 PAut(G) 初等交换.

(3) 若 $w(G)$ 非交换, 则 $G \cong \mathrm{Q}_8 \times \mathrm{C}_2^n$. 显然, $w(G)/Z(G) \cong \mathrm{C}_2 \times \mathrm{C}_2$. 不妨设 $w(G)$ 交换. 对任意的 $w \in w(G)$, 令 $g^w = g^i$, 其中 i 是整数, $(i,p)=1$. 与 (1) 同样的论证可得, $g^w = g^{1+kp^{m-1}}$, 其中 $o(g)=p^m$. 于是 $g^{w^p} = g^{(1+kp^{m-1})^p} = g$. 由此推出 $w^p \in Z(G)$. 从而 $w(G)/Z(G)$ 初等交换. □

注 14.12.17　*注意到定理 14.12.16(1)一般不成立. 例如, 令 $G = \langle a, b \mid a^8 = b^8 = 1, [a,b] = b^4\rangle$. 在 $Z(G)\bigcap \mho_1(G) \cong \mathrm{C}_4 \times \mathrm{C}_4$. 由 [53] 中的推论 6.3.3 可知, $\mathrm{PAut}(G) \cong \mathrm{C}_2 \times \mathrm{C}_2$. 另一方面, [155]中的例 2.3b 和例 2.2 表明, 满足定理 14.12.16 的群是存在的.*

14.13　非中心元的中心化子较小的 p 群

设 G 是群. 则对 G 的每个元素 x 均有 $1 \leqslant \langle x\rangle \leqslant C_G(x) \leqslant G$. 特别地, G 交换当且仅当对所有的 $x \in G$ 都有 $|G : C_G(x)| = 1$. 之后, Ishikawa 在文献 [91] 分类了 $|G : C_G(x)| \leqslant p^2$ 的有限 p 群. 沿着另一方向, 黎先华等在文献 [133] 对于奇素数 p, 分类了所有非中心元 x 满足 $|C_G(x) : \langle x\rangle| \leqslant p^2$ 的有限 p 群. 张丽华等在文献 [264] 分类了所有非中心元 x 满足 $C_G(x)/\langle x\rangle$ 循环的有限 p 群. 王娇等在文献 [221] 进一步推广了文献 [264] 的结果, 他们研究并分类了满足如下条件的 p 群 G: 对 G 中任意非循环的交换子群 H, 只要 $H \nleqslant Z(G)$ 就有 $C_G(H)/H$ 循环. 郝成功等在文献 [80] 分类了含有一个自中心化的循环正规子群的 p 群. 换句话说, 这样的群存在非中心元 x 满足 $|C_G(x) : \langle x\rangle| = 1$ 且 $\langle x\rangle \trianglelefteq G$. 本节介绍他们的工作.

14.13.1　$|C_G(x) : \langle x\rangle| \leqslant p^2$ 的 p 群

称有限 p 群 G 为 k-$\mathcal{NC}$-p 群, 若对 G 的任意非中心的元 x 都有 $|C_G(x) : \langle x\rangle| \leqslant p^k$. 黎先华等在文献 [133] 研究了 k-$\mathcal{NC}$-p 群, 并给出了 $p > 2$ 时 k-$\mathcal{NC}$-p 群的分类.

下面这个引理是简单的, 但它在 p 群研究中经常用到.

引理 14.13.1　*设 G 是一个 p 群, N 和 K 是 G 的两个正规子群. 若 $N < K$ 且 $|K : N| = p$, 则对任意的 $x \in K$ 和 $g \in G$ 都有 $[x, g] \in N$.*

证明　令 $\overline{G} = G/N$. 因为 $|K : N| = p$, 所以 $\overline{K}$ 是 $\overline{G}$ 的一个 p 阶正规子群, 这意味着 $\overline{K} \leqslant Z(\overline{G})$. 从而对任意的 $x \in K$ 和 $g \in G$ 都有 $[\overline{x}, \overline{g}] = 1$. 结论成立. □

引理 14.13.2　*设 G 是非交换 k-$\mathcal{NC}$-p 群. 则*

(i) 若 $H \leqslant G$, 则对任意的 $j \geqslant k$, H 是一个 j-$\mathcal{NC}$-p 群.

(ii) 若 G 存在 p 阶非中心元, 则 $|Z(G)| \leqslant p^k$.

(iii) 若 G 的 p 阶元都在中心中, 则 $\Omega_1(G)$ 同构于 C_p^{k+1} 的一个子群.

证明　(i) 因为对任意的 $x \in H$ 都有 $|C_H(x) : \langle x\rangle| \leqslant |C_G(x) : \langle x\rangle|$, 故 (i) 成立.

(ii) 令 x 是 G 的 p 阶非中心元, 则 $\langle x\rangle\bigcap Z(G)=1$ 且 $\langle x\rangle Z(G)\leqslant C_G(x)$. 因为 G 是一个 k-$\mathcal{NC}$-p 群, 故

$$p^k\geqslant|C_G(x):\langle x\rangle|\geqslant|\langle x\rangle Z(G):\langle x\rangle|=\frac{p\cdot|Z(G)|}{|\langle x\rangle\bigcap Z(G)|\cdot p}=|Z(G)|,$$

结论成立.

(iii) 若 G 的 p 阶元都属于中心, 则 $\Omega_1(G)\leqslant Z(G)$. 所以 $\Omega_1(G)$ 是 G 的初等交换子群. 这意味着对 G 的任意的非中心元 x 都有 $|\langle x\rangle\bigcap\Omega_1(G)|=p$. 于是 $\langle x\rangle\Omega_1(G)\leqslant C_G(x)$. 因为 G 是一个 k-$\mathcal{NC}$-p 群, 故

$$|\Omega_1(G)|/p=|\Omega_1(G)/\langle x\rangle\bigcap\Omega_1(G)|=|\langle x\rangle\Omega_1(G)/\langle x\rangle|\leqslant|C_G(x):\langle x\rangle|\leqslant p^k,$$

从而 $\Omega_1(G)$ 同构于 C_p^{k+1} 的一个子群. □

当 $k=2$ 时, 2-$\mathcal{NC}$-p 群有下列更精细的结论.

定理 14.13.3 设 G 是 2-$\mathcal{NC}$-p 群, 其中 $p>2$. 则

(i) 若 $r_n(G)<3$, 则 $|G|\leqslant p^4$ 或 G 亚循环.

(ii) 若 $r_n(G)\geqslant 3$ 且 $\Omega_1(G)\nleqslant Z(G)$, 则 $|Z(G)|\leqslant p^2$. 进一步地, 若 $|Z(G)|=p$, 则 $|G|\leqslant p^4$; 若 $|Z(G)|=p^2$, 则 $|G|\leqslant p^5$.

(iii) 若 $r_n(G)\geqslant 3$ 且 $\Omega_1(G)\leqslant Z(G)$, 则 $Z(G)=\Omega_1(G)\cong\mathrm{C}_p^3$, 且 $|G|\leqslant p^7$, $\exp(G)=p^2$.

证明 (i) 假设 G 非亚循环, 则 G 为 [26] 中的定理 13.7 的 (b) 型群或者 (c) 型群.

若 G 为 (b) 型群, 则 G 是一个极大类 3 群. 于是 $|Z(G)|=3$ 且 $Z_2(G)$ 为 G 的唯一的 p^2 阶正规子群. 由 [26] 中的定理 9.6(d) 可得, $\Omega_1(G_0)$ 是 G 的一个 3^2 阶初等交换正规子群, 其中 $G_0=C_G(Z_2(G))$. 于是 $Z_2(G)=\Omega_1(G_0)\cong\mathrm{C}_3^2$. 那么存在 3 阶非中心元 $x\in Z_2(G)$ 使得

$$|C_G(Z_2(G)):\langle x\rangle|\leqslant|C_G(x):\langle x\rangle|\leqslant 3^2.$$

于是 $|C_G(Z_2(G))|\leqslant 3^3$. 另一方面, 由 N/C 定理可得, $G/C_G(Z_2(G))\lesssim\mathrm{Aut}(Z_2(G))$. 因为 $Z_2(G)\cong\mathrm{C}_3^2$, 所以 $|\mathrm{Aut}(Z_2(G))|$ 整除 $3(3^2-1)(3-1)$. 从而 $|G/C_G(Z_2(G))|\leqslant 3$. 于是 $|G|\leqslant 3^4$.

若 G 为 (c) 型群, 则 $G=EH$, 其中 $E=\Omega_1(G)\cong\mathrm{M}_p(1,1,1)$, H 是 G 的指数为 p^2 的循环子群. 于是 $Z(G)\bigcap E=Z(E)$ 且 $Z_2(G)\bigcap E>Z(E)$. 取 $x\in(Z_2(G)\bigcap E)-Z(G)$. 则 $o(x)=p$ 且 $|C_G(x)|\leqslant p^3$. 令 $Y=\langle x,Z(E)\rangle$. 则 Y 是 G 的一个 p^2 阶初等交换正规子群. 由 N/C 定理可得, $G/C_G(x)=G/C_G(Y)\lesssim\mathrm{Aut}(Y)$. 于是可得 $|G|\leqslant p^4$.

(ii) 因为 $\Omega_1(G) \nleqslant Z(G)$, 故 G 有 p 阶非中心元. 由 G 是 2-$\mathcal{NC}$-p 群可得 $|Z(G)| \leqslant p^2$. 令 H 是 G 的 p^3 阶初等交换正规子群. 则 $H \nleqslant Z(G)$. 于是存在 G 的 p 阶非中心元 $x \in H$ 使得

$$p^2 \geqslant |C_G(x):\langle x\rangle| \geqslant |HZ(G):\langle x\rangle| = p^2|Z(G):H\bigcap Z(G)|.$$

从而 $C_G(x) = HZ(G)$ 且 $Z(G) = H\bigcap Z(G)$. 也即 $C_G(x) = H$ 且 $Z(G) \leqslant H$. 当 $|Z(G)| = p$ 时, 令 $K = \langle a, Z(G)\rangle$, 其中 $a \in H$ 使得 $aZ(G) \in Z(G/Z(G))$; 当 $|Z(G)| = p^2$ 时, 令 $K = H$. 在这两种取法之下都有 $Z(G) < K \leqslant H\bigcap Z_2(G)$. 于是存在 $x \in K - Z(G)$ 使得 $o(x) = p$ 且对任意的 $g \in G$ 都有 $[x, g] \in Z(G)$, 即存在 $z \in Z(G)$ 使得 $x^g = xz$. 这意味着 $|G:C_G(x)| = |x^G| \leqslant |Z(G)|$, 结论成立.

(iii) 因为 $\Omega_1(G) \leqslant Z(G)$, 故 $\Omega_1(G) = \Omega_1(Z(G)) \cong \mathrm{C}_p^m$. 令

$$Z(G) \cong \mathrm{C}_{p^{r_1}} \times \mathrm{C}_{p^{r_2}} \times \cdots \times \mathrm{C}_{p^{r_m}},$$

其中 $r_1 \geqslant r_2 \geqslant \cdots \geqslant r_m \geqslant 1$. 对任意的 $x \notin Z(G)$ 有 $|Z(G)\bigcap\langle x\rangle| \leqslant p^{r_1}$. 于是

$$p^2 \geqslant |C_G(x):\langle x\rangle| \geqslant |Z(G)\langle x\rangle:\langle x\rangle| = |Z(G):Z(G)\bigcap\langle x\rangle| = p^{r_2+r_3+\cdots+r_m}.$$

从而 $r_2+r_3+\cdots+r_m \leqslant 2$. 注意到 $m \geqslant r_n(G) \geqslant 3$. 由此可得 $m = 3$ 且 $r_2 = r_3 = 1$, 即 $Z(G) \cong \mathrm{C}_{p^{r_1}} \times \mathrm{C}_p \times \mathrm{C}_p$. 从而 $C_G(x) = Z(G)\langle x\rangle$ 且 $|Z(G)\bigcap\langle x\rangle| = p^{r_1}$. 令 $o(x) = p^s$. 则 $s > r_1$. 若 $s > r_1 - 1$, 则 $x^p \notin Z(G)$. 从而有

$$p^2 \geqslant |C_G(x^p):\langle x^p\rangle| \geqslant |Z(G)\langle x\rangle:\langle x^p\rangle| = p\cdot|Z(G):Z(G)\bigcap\langle x\rangle| \geqslant p^3.$$

矛盾. 于是 $o(x) = p^{r_1+1}$ 且 $x^p \in Z(G)$.

假设 $r_1 \geqslant 2$. 因为对任意的 $x \notin Z(G)$ 都有 $o(x) = p^{r_1+1}$ 且 $x^p \in Z(G)$, 故 $Z(G)/\Omega_1(G)$ 是 $G/\Omega_1(G)$ 的唯一的 p^{r_1-1} 阶子群. 由定理 1.10.1 和定理 1.10.2 可得 G 循环. 因为 $\Omega_1(G) \leqslant Z(G)$, 所以 G 交换. 矛盾. 于是 $r_1 = 1$, $Z(G) = \Omega_1(G) \cong \mathrm{C}_p^3$ 且 $\exp(G) = p^2$.

令 $N = Z(G)\langle x\rangle$, 其中 $x \in Z_2(G) - Z(G)$. 则 $o(x) = p^2$ 且 N 是 G 的 p^4 阶交换正规子群. 因为

$$|N| = \frac{|\langle x\rangle|\cdot|Z(G)|}{|\langle x\rangle\bigcap Z(G)|} = p^4 = |C_G(x)|,$$

故 $N = C_G(x)$. 从而 $|G:N| = |x^G|$. 因为 $x \in Z_2(G) - Z(G)$, 所以对任意的 $g \in G$ 都有 $[x, g] \in Z(G)$. 于是存在 $z \in Z(G)$ 使得 $x^g = xz$. 从而 $|G:N| = |x^G| \leqslant |Z(G)| = p^3$. 由此得 $|G| \leqslant p^3\cdot|N| = p^7$. 结论成立. □

下面列出 2-$\mathcal{NC}$-p 群的分类结果, 证明略去.

定理 14.13.4 设 G 是非交换 p 群, 其中 $p>2$. 则 G 是 2-$\mathcal{NC}$-p 群当且仅当 $|G|\leqslant p^4$ 或者 $|G|\geqslant p^5$ 且 G 为下列互不同构的群之一.

(1) $G=\langle a,b \mid a^{p^2}=b^{p^3}=1,[a,b]=b^{p^2}\rangle$;

(2) $G=\langle a,b \mid a^{p^2}=b^{p^3}=1,[a,b]=a^{p}\rangle$;

(3) $G=\langle a,b \mid a^{p^3}=b^{p^3}=1,[a,b]=a^{p^2}\rangle$;

(4) $G=\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=c,[a,c]=[b,c]=1\rangle$;

(5) $G=\langle a,b,c \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=a^p,[a,c]=[b,c]=1\rangle$;

(6) $G=\langle a,b,c \mid a^{p^2}=b^{p^2}=d^{p^2}=1,[a,b]=z_1,[a,d]=z_2,[b,d]=z_3\rangle$, 其中 $z_1,z_2,z_3\in Z(G)$ 且 $Z(G)=\langle z_1\rangle\times\langle z_2\rangle\times\langle z_3\rangle=\langle a^p\rangle\times\langle b^p\rangle\times\langle c^p\rangle\cong \mathrm{C}_p^3$;

(7) $G=\langle x,a,b,c,d\rangle$, 其中 x, a, b, c, d 满足 $b^p=c^p=d^p=1$, $x^p=c^{s_1}d^{t_1}, a^p=c^{u_1}d^{v_1}$, $[x,a]=b$, $[x,b]=d$, $[a,b]=c$, $\langle c\rangle\times\langle d\rangle=Z(G)$, 其中 $0\leqslant s_1,t_1,u_1,v_1\leqslant p-1$;

(8) $G=\langle x,a,b,c,d\rangle$, 其中 x, a, b, c, d 满足 $b^p=c^p=d^p=1$, $x^p=c^{s_2}d^{t_2}, a^p=c^{u_2}d^{v_2}$, $[x,a]=1$, $[x,b]=d$, $[a,b]=c$, $\langle c\rangle\times\langle d\rangle=Z(G)$, 其中 $0\leqslant s_2,t_2,u_2,v_2\leqslant p-1$.

14.13.2 $C_G(x)/\langle x\rangle$ 循环的 p 群及其推广

有限 p 群 G 称为 $\mathcal{P}$ 群, 若 G 的非中心元 x 均满足 $C_G(x)/\langle x\rangle$ 循环. 有限 p 群 G 称为 $\mathcal{CAC}$ 群, 若对 G 中任意非循环的交换子群 H, 只要 $H\nleqslant Z(G)$ 就有 $C_G(H)/H$ 循环. 本节的目的就是分类 $\mathcal{P}$ 群和 $\mathcal{CAC}$ 群. 内容取自文献 [221], [264].

引理 14.13.5 若 G 是 $\mathcal{P}$ 群, 则 $r(G)\leqslant 2$.

证明 若否, 则存在 $A\leqslant G$ 使得 $A\cong \mathrm{C}_p^3$. 若 $A\nleqslant Z(G)$, 则存在 $x\in A\setminus Z(G)$. 因为 A 交换, 故 $A\leqslant C_G(x)$. 又因为 $A/\langle x\rangle\cong \mathrm{C}_p^2$, 故 $C_G(x)/\langle x\rangle$ 不循环. 这与假设矛盾. 若 $A\leqslant Z(G)$, 则对所有的 $x\in G\setminus Z(G)$ 均有 $A\langle x\rangle/\langle x\rangle\leqslant C_G(x)/\langle x\rangle$. 因为 $A\langle x\rangle/\langle x\rangle\cong A/A\bigcap\langle x\rangle\cong \mathrm{C}_p^2$ 或 C_p^3, 故 $C_G(x)/\langle x\rangle$ 不循环. 也与假设矛盾. □

引理 14.13.6 设 G 是亚循环的非交换 p 群, $p>2$. 则 G 是 $\mathcal{P}$ 群当且仅当 G 是 $\mathcal{A}_1$ 群.

证明 $\Longleftarrow$: 令 $x\in G\setminus Z(G)$. 由定理 1.7.7 可知, $Z(G)=\Phi(G)$. 因为 $\Phi(C_G(x))\leqslant\Phi(G)$, 故 $x\notin\Phi(C_G(x))$. 又因为 G 亚循环, 故 $C_G(x)$ 也亚循环. 从而 $d(C_G(x))\leqslant 2$. 由此可得, 存在 $y\in G$ 使得 $C_G(x)=\langle x,y\rangle$. 因而 $C_G(x)/\langle x\rangle$ 循环. 即 G 是 $\mathcal{P}$ 群.

$\Longrightarrow$: 因为 G 是奇数阶亚循环群, 故 $\Omega_1(G)\cong \mathrm{C}_p^2$. 令 $G=\langle a,b\rangle$ 且 $H=\langle a\rangle\Omega_1(G)$, 其中 $\langle a\rangle\lhd G$. 则 $H'\leqslant\langle a\rangle\bigcap\Omega_1(G)$. 特别地, $|H'|\leqslant p$. 于是 $\langle a^p\rangle\Omega_1(G)$ 交换. 因而 $H\leqslant C_G(a^p)$. 因为 G 是 $\mathcal{P}$ 群且 $H/\langle a^p\rangle=H/\mho_1(H)\cong \mathrm{C}_p^2$, 有 $a^p\in Z(G)$. 再由 G 是奇数阶亚循环群可得 G 正则. 因而 $[a,b]^p=1$ 等价于 $[a^p,b]=1$. 由此可得 $|G'|=p$. 由定理 1.7.7 可知, G 是 $\mathcal{A}_1$ 群. □

显而易见, 引理 14.13.6 的论证对于通常亚循环 2 群也成立.

推论 14.13.7　设 G 是通常亚循环 2 群. 则 G 是 $\mathcal{P}$ 群当且仅当 G 是 $\mathcal{A}_1$ 群.

引理 14.13.8　设 G 是 $\mathcal{P}$ 群且 H 是 G 的非交换子群. 则 H 也是 $\mathcal{P}$ 群.

证明　若否, $\forall x \in H \setminus Z(H)$ 我们有 $x \notin Z(G)$. 则 $x \in Z(G) \bigcap H \leqslant Z(H)$, 矛盾. 于是 $x \in G \setminus Z(G)$. 因为 G 是 $\mathcal{P}$ 群, 故 $C_G(x)/\langle x\rangle$ 循环. 因为 $C_H(x) \leqslant C_G(x)$, 故 $C_H(x)/\langle x\rangle$ 也循环. □

定理 14.13.9　设 p 是奇素数. 则 G 是 $\mathcal{P}$ 群当且仅当 G 是下列互不同构的群之一.

(1) p^n 阶的亚循环内交换群, 其中 $n > 3$;

(2) $\mathrm{M}_p(1,1,1)$;

(3) $G = \langle a, b, c \mid a^9 = c^3 = 1, b^3 = a^3, [a,b] = c, [c,a] = 1, [c,b] = a^{-3}\rangle$;

(4) $G \cong \mathrm{M}_p(1,1,1) * \mathrm{C}_{p^{n-2}}$, 其中 $n > 2$;

(5) $G = \langle a, x, y \mid a^{p^{n-2}} = 1, x^p = y^p = 1, [a,x] = y, [x,y] = a^{ip^{n-3}}, [y,a] = 1\rangle$, $i = 1$ 或 σ, 其中 σ 是一个固定的模 p 的平方非剩余.

证明　若 $|G| \leqslant p^4$, 则通过对 p^3 阶和 p^4 阶群的群表的简单的检查即得结论. 设 $|G| \geqslant p^5$. 由引理 14.13.5 可知 $r(G) \leqslant 2$. 于是 $r_n(G) \leqslant 2$. 若 $r_n(G) = 1$, 则 G 循环, 矛盾. 故 $r_n(G) = 2$. 正规秩 $r_n(G)$ 为 2 的群已被 Blackburn 在 [31] 中的定理 4.1 分类. 它们是下列互不同构的群之一.

(i) 亚循环群;

(ii) $\mathrm{M}_p(1,1,1) * \mathrm{C}_{p^{n-2}}$;

(iii) 阶 $\geqslant 3^5$ 的极大类 3 群;

(iv) $\langle a, x, y \mid a^{p^{n-2}} = 1, x^p = y^p = 1, [a,x] = y, [x,y] = a^{ip^{n-3}}, [y,a] = 1\rangle$, $i = 1$ 或 σ, 其中 σ 是一个固定的模 p 的平方非剩余.

若 G 是群 (i), 由引理 7.2.1 即得群 (1).

若 G 是群 (ii), 则 $Z(G)$ 是 p^2 阶循环子群. 令 $g \in G \setminus Z(G)$. 则 $C_G(g) < G$. 明显地, $C_G(g) \geqslant \langle g\rangle Z(G)$. 于是 $C_G(g) = \langle g\rangle Z(G)$. 因而 $C_G(g)/\langle g\rangle \cong Z(G)/Z(G) \bigcap \langle g\rangle$ 是循环的, 即 G 是 $\mathcal{P}$ 群. 这是群 (4).

若 G 是群 (iii), 由 [30] 中的定理 2.6 和定理 1.11.8 可知, 基本子群 G_1 是交换群或非交换的亚循环群. 因为 $|G| \geqslant 3^5$, 故 $|G_1| \geqslant 3^4$. 由此可得, 存在 $H \trianglelefteq G$ 使得 $|H| = 3^4$, $d(H) \geqslant 2$ 且 H 是交换群或非交换的亚循环群. 由引理 14.13.5 得 $d(H) = 2$. 再由定理 1.11.8 可知, $\mho_1(H) \ncong \mathrm{C}_9$. 因而 $H \cong \mathrm{C}_9^2$ 或 $\mathrm{M}_3(2,2)$. 于是 $\mho_1(H) \leqslant Z(H)$ 且 $\mho_1(H) \cong \mathrm{C}_3^2$. 因为 G 是极大类的, 故 $|Z(G)| = 3$. 从而存在 $x \in \mho_1(H) \setminus Z(G)$. 因为 H 不循环, 故 $H/\langle x\rangle$ 也不循环. 现在由 $H \leqslant C_G(x)$ 可得, $C_G(x)/\langle x\rangle$ 不循环. 即 G 不是 $\mathcal{P}$ 群.

若 G 是群 (iv), 计算可知, $Z(G) = \langle a^p\rangle$ 是一个指数为 p^3 的子群且 $\langle a, y\rangle$ 是交换极大子群. 因为 $|G'| = p^2$, 由 [26] 中的 §1, 练习 69(a) 可知, G 有唯一的交

换极大子群. 令 $g \in G \setminus Z(G)$. 则 $\langle a^p, g\rangle \leqslant C_G(g) < G$. 若 $C_G(g) = \langle a^p, g\rangle$, 则 $C_G(g)/\langle g\rangle$ 循环. 若 $C_G(g) > \langle a^p, g\rangle$, 则 $C_G(g) \lessdot G$. 因为 $\langle a^p, g\rangle \leqslant Z(C_G(g))$ 且 $|C_G(g)/\langle a^p, g\rangle| = p$, 故 $C_G(g)$ 交换. 于是 $C_G(g) = \langle a, y\rangle$ 且 $g = a^i y^j$, 其中 $(i,p)=1$ 或 $(j,p)=1$. 由此可得 $C_G(g)/\langle g\rangle$ 循环. 即 G 是 $\mathcal{P}$ 群. 这是群 (5). □

下面我们分类偶数阶的 $\mathcal{P}$ 群.

引理 14.13.10 设 G 是 2^n 阶的 $\mathcal{P}$ 群, $n \geqslant 5$, $M \lessdot G$. 若 M 是极大类的, 则 G 也是极大类的.

证明 若否, 由 [26] 中的定理 9.10 可知, $G/G' \cong C_p^3$. 由此可得

$$\mho_1(G) = G' = M' = \mho_1(M).$$

因而 $\exp(G) = \exp(M)$. 因为 M 是极大类的, 由极大类 2 群的分类可知, M 有一个极大子群 H 是循环的. 令 $K = \Omega_2(H)$. 则 $K \cong C_4$ 且 K char H char $M \trianglelefteq G$. 因而 $K \trianglelefteq G$. 由 N/C 定理可得

$$G/C_G(K) \lesssim \mathrm{Aut}(K) \cong C_2.$$

再由 M 是极大类的, 故 $|Z(M)| = 2$. 因而 $K \nleqslant Z(M)$. 于是 $G/C_G(K) \cong C_2$. 因为 G 不是极大类的, 故 $C_G(K)$ 不循环. 又 $n \geqslant 5$, 故

$$K \leqslant \mho_1(M') \leqslant \Phi(C_G(K)).$$

由此可得 $C_G(K)/K$ 不循环. 这与 G 是 $\mathcal{P}$ 矛盾. □

引理 14.13.11 设 G 是 2^n 阶的 $\mathcal{P}$ 群, $n \geqslant 6$, $M \lessdot G$ 且 $M = \langle a, b, c \mid a^{2^{n-4}} = b^{2^2} = 1, c^2 = a^2b^2, [a,b] = b^2, [c,a] = [c,b] = 1\rangle$. 则

(1) $Z(M) = \langle a^2, c\rangle = \langle b^2, c\rangle \cong C_2 \times C_{2^{n-4}}$, $\Omega_1(M) = \langle a^{2^{n-5}}, b^2\rangle \cong C_2^2$;

(2) $\Phi(G) = \mho_1(G) \leqslant Z(M) \leqslant Z(G)$;

(3) $G' \leqslant \Omega_1(Z(M)) = \Omega_1(M)$;

(4) $M = \Omega_{n-4}(G)$, 特别地, 对所有的 $x \in G \setminus M$ 都有 $o(x) = 2^{n-3}$.

证明 (1) 结论显然成立.

(2) 首先可证: $Z(M) \leqslant Z(G)$. 若否, 如果 $a^2 \notin Z(G)$, 则由 G 是 $\mathcal{P}$ 群可得 $C_G(a^2)/\langle a^2\rangle$ 循环. 因为 $C_G(a^2) \geqslant M$, 故 $M/\langle a^2\rangle$ 循环. 矛盾. 因而 $a^2 \in Z(G)$. 类似地, $c \in Z(G)$.

再证对所有的 $x \in G$ 都有 $x^2 \in Z(M)$. 因为 $x^2 \in M$, 只需证 $x^2 \in Z(G)$. 若否, 由 $C_G(x^2)/\langle x^2\rangle \geqslant Z(M)\langle x\rangle/\langle x^2\rangle$ 和 G 是 $\mathcal{P}$ 群可得, $Z(M)\langle x\rangle/\langle x^2\rangle$ 循环. 因为 $\langle x^2\rangle \leqslant \Phi(Z(M)\langle x\rangle)$, 故 $Z(M)\langle x\rangle$ 循环. 特别地, $Z(M)$ 循环. 矛盾.

(3) 由 (2) 所证可知, $G/Z(G)$ 初等交换. 于是 G' 初等交换. 特别地, $G' \leqslant \Omega_1(Z(M)) = \Omega_1(M)$.

(4) 若否, 则 $\Omega_{n-4}(G)=G$. 由 (2) 和 (3) 可得 G 是 4 交换的. 因为 $n-4\geqslant 2$, 故 $\exp(G)=\exp(\Omega_{n-4}(G))=2^{n-4}$. 因而 $\exp(\mho_1(G))=2^{n-5}$. 由此可得

$$\Phi(G)=\mho_1(G)\leqslant \Omega_{n-5}(Z(M))=\langle b^2,c^2\rangle=\Phi(M).$$

于是 $d(G)=d(M)+1=4$.

取 $x\in G\setminus M$. 则 $\langle a,b,c,x\rangle=G$. 因为

$$G'\leqslant \Omega_1(M)=\langle a^{2^{n-5}},b^2\rangle,$$

故 $[a,x]\in\langle a^{2^{n-5}}\rangle$ 或 $[a,bx]\in\langle a^{2^{n-5}}\rangle$. 不妨设 $[a,x]\in\langle a^{2^{n-5}}\rangle$. 若 $[a,x]=1$, 则

$$C_G(a)/(\langle a\rangle\Phi(G))\geqslant\langle\bar{c},\bar{x}\rangle\cong \mathrm{C}_2^2.$$

因而 $C_G(a)/\langle a\rangle$ 非循环. 矛盾. 故 $[a,x]=a^{2^{n-5}}$.

注意到 $c\in Z(G)$ 且 $[a,x]=[a,xc^i]$, 其中 i 是整数. 因为

$$x^2\in\Phi(G)=\langle b^2,c^2\rangle,$$

故对某个适当的 i 有 $(xc^i)^2=c^2$ 或 $(xc^i)^2=c^2b^2=a^2$. 不妨设 $x^2=c^2$ 或 a^2. 若 $x^2=c^2$, 则 $o(xc^{-1})=2$. 若 $x^2=a^2$, 则 $o(xa^{-1+2^{n-6}})=2$. 这说明在任何情况下, 存在一个对合 $y\in G\setminus M$. 因而 $\langle y\rangle\Omega_1(M)\cong\mathrm{C}_2^3$, 这与引理 14.9.1 矛盾. □

引理 14.13.12 *G 和 M 如引理 14.13.11所设. 则 G 是下列不同构的群之一.*

(1) $\langle a,b,c\mid a^{2^{n-3}}=b^{2^2}=1,c^2=a^2b^2,[a,b]=b^2,[c,a]=[c,b]=1\rangle$;

(2) $\langle a,b,c\mid a^{2^{n-3}}=b^{2^2}=1,c^2=a^2b^2,[a,b]=b^2,[c,a]=a^{2^{n-4}},[c,b]=1\rangle$.

证明 由引理 14.13.11(4) 可得, $\exp(G)=2^{n-3}$ 且对所有的 $x\in G\setminus M$ 都有 $o(x)=2^{n-3}$. 又由引理 14.13.11(2) 得, $x^2\in Z(M)=\langle b^2,c\rangle$. 于是可设 $x^2=c$ 或 $x^2=cb^2$. 再由引理 14.13.11(3) 得, $G'\cong\mathrm{C}_2$ 或 $G'\cong\mathrm{C}_2^2$.

若 $G'\cong\mathrm{C}_2$, 则 $G'=M'=\langle b^2\rangle$. 若 $[b,x]=1$ 且 $[a,x]=1$, 令 $a_1=ax^{-1}$. 则

$$a_1^{2^{n-3}}=1,\quad [a_1,b]=[ax^{-1},b]=[a,b]=b^2,\quad a_1^2b^2=x^2.$$

因而

$$G=\langle a_1,b,x\mid a_1^{2^{n-3}}=b^{2^2}=1,x^2=a_1^2b^2,[a_1,b]=b^2,[x,a_1]=[x,b]=1\rangle.$$

此时 G 同构于群 (1). 若 $[b,x]=1$ 且 $[a,x]=b^2$, 令 $x_1=bx$. 则 $[b,x_1]=1$ 且 $[a,x_1]=1$. 若 $[b,x]=b^2$, 令 $x_1=ax$. 则 $[b,x_1]=1$. 在这两种情况下, G 都同构于群 (1).

若 $G' \cong \mathrm{C}_2^2$, 则 $G' = \Omega_1(M)$. 我们考虑 $[b,x]$ 的可能取值.

情形 1 $[b,x]=1$.

在这种情形下, $[a,x]=a^{2^{n-5}}$ 或 $[a,x]=a^{2^{n-5}}b^2$.

若 $[a,x]=a^{2^{n-5}}$, 令 $a_1 = ax^{-1+2^{n-5}}$. 则

$$a_1^{2^{n-3}}=1, \quad x^2=a_1^2b^2, \quad [a_1,b]=[ax^{-1+2^{n-5}},b]=[a,b]=b^2,$$

$$[a_1,x]=[ax^{-1+2^{n-5}},x]=[a,x]=a^{2^{n-5}}=a_1^{2^{n-4}}.$$

于是 $G=\langle a,b,x\rangle=\langle a_1,b,x\rangle$ 具有如上的定义关系. 因而 G 同构于群 (2).

若 $[a,x]=a^{2^{n-5}}b^2$, 令 $x_1=bx$. 则 $[b,x_1]=1$ 且 $[a,x_1]=a^{2^{n-5}}$. 此时转化为 $[a,x]=a^{2^{n-5}}$ 的情形.

情形 2 $[b,x]=b^2$.

令 $x_1=ax$. 则 $[b,x_1]=1$. 这化归为情形 1.

情形 3 $[b,x]=a^{2^{n-5}}$.

若 $[a,x]=1$, 令 $a_1=ax^{-1}$, $b_1=bx^{2^{n-5}}$, $x_1=x^{1+2^{n-5}}$. 计算可得

$$o(a_1)=2^{n-3}, \quad o(b_1)=2^2, \quad [a_1,b_1]=b^2x^{2^{n-4}}=b_1^2,$$

$$[a_1,x_1]=1, \quad [b_1,x_1]=x_1^{2^{n-4}}, \quad a_1^2b_1^2=x_1^2.$$

于是 $G=\langle a,b,x\rangle=\langle a_1,b_1,x_1\rangle$ 具有如上的定义关系. 此时 G 同构于群 (2).

若 $[a,x]=b^2$, 令 $a_1=a$, $x_1=bx$. 若 $[a,x]=a^{2^{n-5}}$, 令 $a_1=ab$, $x_1=x$. 若 $[a,x]=a^{2^{n-5}}b^2$, 令 $a_1=ab$, $x_1=bx$. 在这三种情形下, 有 $[a_1,x_1]=1$, $[b,x_1]=a_1^{2^{n-5}}$. 此时转化为 $[a,x]=1$ 的情形.

情形 4 $[b,x]=a^{2^{n-5}}b^2$.

令 $x_1=ax$. 则 $[b,x_1]=a^{2^{n-5}}$. 这化归为情形 3. □

引理 14.13.13 *设 G 是 2^n 阶的 $\mathcal{P}$ 群, $n \geqslant 6$, $M \lessdot G$ 且 $M=\langle a,b,c \mid a^{2^{n-4}}=b^{2^2}=1, c^2=a^2b^2, [a,b]=b^2, [c,a]=a^{2^{n-5}}, [c,b]=1\rangle$. 则 $n=6$ 且 $G\cong\langle a,b,c,d \mid a^4=b^4=1, c^2=a^2b^2, b^2=d^2, [a,b]=b^2, [a,c]=a^2, [a,d]=1, [b,c]=1, [b,d]=a^2, [c,d]=c^2\rangle$.*

证明 类似于引理 14.13.11 的证明, 我们有

(1) $\Phi(M)=Z(M)=\langle a^2,b^2\rangle\cong \mathrm{C}_2\times\mathrm{C}_{2^{n-5}}$, $\Omega_1(M)=M'=\langle a^{2^{n-5}}, b^2\rangle\cong\mathrm{C}_2^2$;

(2) $\Phi(G)=\Phi(M)=Z(M)\leqslant Z(G)$, 特别地, $d(G)=4$, $\exp(G)=2^{n-4}$;

(3) $G'=\Omega_1(Z(M))=\Omega_1(M)=M'$;

(4) $G\setminus M$ 没有 2 阶元.

注意到 $[a,M]=M'=G'$, 取适当的 $d\in G\backslash M$ 使得 $[a,d]=1$. 则 $G=\langle a,b,c,d\rangle$. 设 $d^2=a^{2i}b^{2j}$, 其中 i 和 j 是整数. 用 da^{-i} 替换 d, 可设 $d^2=b^{2j}$. 由 (4) 可知, $j\neq 0$. 因而 $d^2=b^2$.

若 $[b,d]\in\langle b^2\rangle$, 则 $[b,d]=1$ 或 $[b,ad]=1$. 因而 $|C_G(b)/(\langle b\rangle\Phi(G))|\geqslant 4$. 这与 G 是 $\mathcal{P}$ 群矛盾. 于是 $[b,d]=a^{2^{n-5}}$ 或 $a^{2^{n-5}}b^2$. 类似地, $[c,d]=b^2$ 或 $b^2a^{2^{n-5}}$.

若 $n\geqslant 7$, 则 $a^{2^{n-6}}\in\mho_1(G)\leqslant Z(G)$. 因而 $(bda^{2^{n-6}})^2=(bd)^2a^{2^{n-5}}=[b,d]a^{2^{n-5}}$. 由 (4) 可知, $[b,d]a^{2^{n-5}}\neq 1$. 于是 $[b,d]=b^2a^{2^{n-5}}$. 由此可得 $(abcd)^2=b^2[c,d]$. 再由 (4) 可知, $b^2[c,d]\neq 1$. 于是 $[c,d]=b^2a^{2^{n-5}}=[b,d]$. 因而 $[bc,d]=1$. 由此得 $|C_G(d)/(\langle d\rangle\Phi(G))|\geqslant 4$. 这与 G 是 $\mathcal{P}$ 群矛盾. 因而 $n=6$.

又由 (4), $1\neq(abd)^2=a^2b^2[b,d]$. 因而 $[b,d]=a^2$. 再由 (4) 得, $1\neq(bcd)^2=b^2[c,d]$. 因而 $[c,d]=b^2a^2=c^2$, 我们得到所希望的群 G. □

引理 14.13.14　*设 G 是 2^n 阶的 $\mathcal{P}$ 群, $n\geqslant 5$, $M\lessdot G$ 且 $M=\langle a,b,c\mid a^{2^{n-3}}=b^2=c^2=1,[c,b]=a^{2^{n-4}},[b,a]=[c,a]=1\rangle\cong \mathrm{D}_8*\mathrm{C}_{2^{n-3}}$. 则 $G\cong \mathrm{D}_8*\mathrm{C}_{2^{n-2}}$.*

证明　类似于引理 14.13.11 的证明, 我们有

(1) $Z(M)=\langle a\rangle\cong \mathrm{C}_{2^{n-3}}$, $\Omega_1(Z(M))=\langle a^{2^{n-4}}\rangle$;

(2) $\Phi(G)=\mho_1(G)\leqslant Z(M)\leqslant Z(G)$, 特别地, $\exp(G)\leqslant 2^{n-2}$;

(3) $G'=\Omega_1(Z(M))=M'$;

(4) $M=\Omega_{n-3}(G)$, 特别地, 对所有的 $x\in G\setminus M$ 都有 $o(x)=2^{n-2}$.

由 (4) 可设 $x^2=a$. 考虑 $[b,x]$ 和 $[c,x]$. 若 $[b,x]=1$ 且 $[c,x]=1$, 则 $G=\langle b,c\rangle*\langle x\rangle\cong \mathrm{D}_8*\mathrm{C}_{2^{n-2}}$. 若 $[b,x]=1$ 且 $[c,x]=a^{2^{n-4}}$, 令 $x_1=bx$, 则 $[b,x_1]=1$ 且 $[c,x_1]=[c,bx]=1$. 于是 $G=\langle b,c\rangle*\langle x_1\rangle\cong \mathrm{D}_8*\mathrm{C}_{2^{n-2}}$. 若 $[b,x]=a^{2^{n-4}}$, 令 $x_1=cx$, 则 $[b,x_1]=1$. 这化归为 $[b,x]=1$ 的情形. □

引理 14.13.15　*设 G 是 2^6 阶的 $\mathcal{P}$ 群. 则 G 没有子群 $M\cong\langle a,b,c\mid a^4=c^4=1,a^2=b^2,[a,b]=a^2,[c,a]=c^2,[c,b]=1\rangle$.*

证明　若否, 类似于引理 14.13.11 的证明, 我们有

(1) $\Phi(M)=Z(M)=\Omega_1(M)=M'=\langle a^2,c^2\rangle\cong \mathrm{C}_2^2$;

(2) $\Phi(G)=\Phi(M)=Z(M)\leqslant Z(G)$, 特别地, $d(G)=4$ 且 $\exp(G)=4$;

(3) $G'=\Omega_1(Z(M))=\Omega_1(M)=M'$;

(4) $G\setminus M$ 没有 2 阶元.

注意到 $[a,M]=M'=G'$. 取适当的 $x\in G\setminus M$ 使得 $[a,x]=1$. 不妨设 $x^2=c^2$. 类似于引理 14.13.13 的论证可得, $[b,x]=c^2$ 或 a^2c^2, $[c,x]=a^2$ 或 a^2c^2.

由 (4) 可得, $1\neq(abx)^2=a^2c^2[b,x]$ 且 $1\neq(acx)^2=a^2c^2[c,x]$. 因而 $[b,x]=c^2$ 且 $[c,x]=a^2$. 由此可得 $(abcx)^2=1$. 与 (4) 矛盾. □

引理 14.13.16　*设 G 是 2^7 阶的 $\mathcal{P}$ 群. 则 G 没有子群 $M\cong\langle a,b,c,d\mid a^4=b^4=1,c^2=a^2b^2,b^2=d^2,[a,b]=b^2,[a,c]=a^2,[a,d]=1,[b,c]=1,[b,d]=a^2,[c,d]=$*

$c^2\rangle$.

证明 若否, 类似于引理 14.13.11 的证明, 我们有

(1) $\Phi(M)=Z(M)=\Omega_1(M)=M'=\langle a^2,b^2\rangle\cong \mathrm{C}_2^2$;

(2) $\Phi(G)=\Phi(M)=Z(M)\leqslant Z(G)$, 特别地, $d(G)=5$ 且 $\exp(G)=4$;

(3) $G'=\Omega_1(Z(M))=\Omega_1(M)=M'$.

注意到 $[a,M]=M'=G'$. 取适当的 $x\in G\setminus M$ 使得 $[a,x]=1$. 因而 $C_G(a)/(\langle a\rangle\Phi(G))\geqslant\langle\bar{d},\bar{x}\rangle\cong \mathrm{C}_2^2$. 这与 G 是 $\mathcal{P}$ 群矛盾. □

定理 14.13.17 *设 G 是 2^n 阶群. 则 G 是 $\mathcal{P}$ 群当且仅当 G 是下列互不同构的群之一.*

(1) 亚循环的内交换 p 群;

(2) 极大类 2 群;

(3) $\mathrm{D}_8*\mathrm{C}_{2^{n-2}}$;

(4) $\langle a,b,c\mid a^{2^{n-3}}=b^{2^2}=1,c^2=a^2b^2,[a,b]=b^2,[c,a]=[c,b]=1\rangle$;

(5) $\langle a,b,c\mid a^{2^{n-3}}=b^{2^2}=1,c^2=a^2b^2,[a,b]=b^2,[c,a]=a^{2^{n-4}},[c,b]=1\rangle$;

(6) $\mathrm{Q}_8\times\mathrm{C}_2$;

(7) $\langle a,b,c\mid a^4=c^4=1,a^2=b^2,[a,b]=a^2,[c,a]=c^2,[c,b]=1\rangle$;

(8) $\langle a,b,c,d\mid a^4=b^4=1,c^2=a^2b^2,b^2=d^2,[a,b]=b^2,[a,c]=a^2,[a,d]=1,[b,c]=1,[b,d]=a^2,[c,d]=c^2\rangle$.

证明 若 $n\leqslant 5$, 则由阶 $\leqslant 2^5$ 的分类可知结论成立. 下设 $n\geqslant 6$ 且 G 是 $\mathcal{P}$ 群.

由归纳假设, G 的每个极大子群是交换的或同构于群 (1)—(5),(7) 和 (8) 之一. 若 G 有一个极大子群同构于群 (2)—(5), (7) 和 (8), 由引理 14.13.10 — 引理 14.13.16 可知, G 同构于群 (2)—(5) 和 (8).

设 G 的每个极大子群是交换的或是亚循环的内交换的. 由引理 14.13.5 可知, G 的每个极大子群是亚循环的. 若 G 非亚循环, 则 G 内亚循环. 由定理 8.1.1 可知 $|G|\leqslant 2^5$. 这与 $|G|\geqslant 2^6$ 矛盾. 故 G 是亚循环的.

若 G 是内交换的, 则 G 为群 (1).

若 G 不内交换, 则 G 是亚循环的 $\mathcal{A}_2$ 群. 从而 $|G'|=4$. 设 $G=\langle a,b\rangle$, 其中 $G'<\langle a\rangle$. 则 $o(a)\geqslant 8$ 且 $a^t\in Z(G)$ 当且仅当 $4|t$. 因而 $a^2\notin Z(G)$. 因为 $|G|\geqslant 2^6$ 且 $|G'|=4$, G 没有循环极大子群. 于是 $C_G(a^2)=\langle a,b^2\rangle$ 非循环. 注意到 $\langle a^2\rangle\leqslant\mho_1(C_G(a^2))$. 故 $C_G(a^2)/\langle a^2\rangle$ 非循环. 这与 G 是 $\mathcal{P}$ 群矛盾.

显而易见, 定理中的群互不同构. 下证定理中的群是 $\mathcal{P}$ 群.

若 G 是群 (1), 由推论 14.13.7 可知 G 是 $\mathcal{P}$ 群.

若 G 是群 (2), 则 G 有一个循环极大子群且由极大类 2 群的分类可知, G 是亚循环的. 令 $\langle a\rangle$ 是 G 的一个循环极大子群. 则 $\Phi(G)=\langle a^2\rangle$ 且 $Z(G)=\langle a^{2^{n-2}}\rangle$. 令 $x\in G\setminus Z(G)$. 若 $x\notin\Phi(G)$, 则 $x\notin\Phi(C_G(x))$. 因为 G 亚循环, 故 $C_G(x)$ 亚循环. 因

而 $d(C_G(x)) \leqslant 2$. 于是存在 $y \in G$ 使得 $C_G(x) = \langle x, y\rangle$. 由此可得 $C_G(x)/\langle x\rangle = \langle \bar{y}\rangle$. 若 $x \in \Phi(G) \setminus Z(G)$, 则 $C_G(x) = \langle a\rangle$. 明显地, $C_G(x)/\langle x\rangle$ 循环. 故 G 是 $\mathcal{P}$ 群.

若 G 是群 (3–7), 则 $|G:Z(G)| \leqslant 8$. 由此可得对所有的 $x \in G \setminus Z(G)$ 都有 $|G:\langle x, Z(G)\rangle| \leqslant 4$. 注意到 $\langle x, Z(G)\rangle \leqslant Z(C_G(x))$ 且 $C_G(x) < G$. 则 $|C_G(x)/Z(C_G(x))| \leqslant 2$. 因而 $C_G(x)$ 交换. 简单的验证可知 $r(G)=2$. 因而 $d(C_G(x)) \leqslant 2$. 于是存在 $y \in G$ 使得 $C_G(x) = \langle x, y\rangle$. 从而 $C_G(x)/\langle x\rangle = \langle \bar{y}\rangle$.

若 G 是群 (8), 则 $Z(G) = \Phi(G) = \Omega_1(G) \cong C_2^2$. 验证易得对所有的 32 阶群 M 均有 $Z(M) = Z(G)$. 因为对所有的 $x \in G \setminus M$ 均有 $Z(C_G(x)) \geqslant \langle x, Z(G)\rangle$, 故 $Z(C_G(x)) > Z(G)$. 于是 $|C_G(x)| \leqslant 16$. 由此可得 $C_G(x)$ 交换, 从而 $d(C_G(x)) \leqslant 2$. 于是存在 $y \in G$ 使得 $C_G(x) = \langle x, y\rangle$. 从而 $C_G(x)/\langle x\rangle = \langle \bar{y}\rangle$. □

王娇等在文献 [221] 中分类了比 $\mathcal{P}$ 群更广的一类 p 群, 即 $\mathcal{CAC}$ 群. 以下内容取自 [221].

定理 14.13.18 *设 G 是有限非交换 p 群. 若 G 是 $\mathcal{P}$ 群, 则 G 是 $\mathcal{CAC}$ 群.*

证明 设 H 为 G 的任意非循环交换子群, 且 $H \nleqslant Z(G)$. 则存在 $x \in H \setminus Z(G)$. 由定理条件, 有 $C_G(x)/\langle x\rangle$ 循环, 从而 $C_G(x)$ 交换, 进而 $H \trianglelefteq C_G(x)$. 于是 $C_G(x)/H$ 循环. 又由 $C_G(H) \leqslant C_G(x)$, 有 $C_G(H)/H$ 循环. □

下面这个例子说明存在有限非交换 p 群 G, 它是 $\mathcal{CAC}$ 群但不是 $\mathcal{P}$ 群.

例 14.13.19 *设 $G = \langle a, b, c \mid a^4 = b^4 = c^2 = 1, [b, a] = c, [c, a] = [c, b] = 1\rangle$. 易知 G 是 $\mathcal{CAC}$ 群. 显然, $a \notin Z(G)$, 但 $C_G(a)/\langle a\rangle = \langle a, b^2, c\rangle/\langle a\rangle$ 非循环, 即不是 $\mathcal{P}$ 群.*

显然交换 p 群均为 $\mathcal{CAC}$ 群. 下面所述的 $\mathcal{CAC}$ 群均指非交换的 $\mathcal{CAC}$ 群.

首先给出 $\mathcal{CAC}$ 群的某些性质.

定理 14.13.20 *若 G 为 $\mathcal{CAC}$-p-群, 则 $r(G) \leqslant 3$.*

证明 若否, 则存在 $A \leqslant G$ 且 $A \cong C_p^4$. 若 $A \nleqslant Z(G)$, 则存在 $a \in A \setminus Z(G)$, $b \in A$ 使得 $\langle a, b\rangle$ 非循环. 由 A 交换, 有 $A \leqslant C_G(\langle a, b\rangle)$. 又因为 $A/\langle a, b\rangle$ 非循环, 于是 $C_G(\langle a, b\rangle)/\langle a, b\rangle$ 非循环. 与 G 为 $\mathcal{CAC}$ 群矛盾. 若 $A \leqslant Z(G)$, 则任取 $x \in G \setminus Z(G)$, 存在 $c \in A$ 使得 $\langle c, x\rangle$ 非循环. 由 $\langle A, x\rangle \leqslant C_G(\langle c, x\rangle)$ 且 $\langle A, x\rangle/\langle c, x\rangle$ 非循环可知, $C_G(\langle c, x\rangle)/\langle c, x\rangle$ 非循环, 同样得到矛盾. □

引理 14.13.21 *设 G 为 $\mathcal{CAC}$ 群, $r(G) = 3$, $A \leqslant G$, 且 $A \cong C_p^3$. 若 $A \nleqslant Z(G)$, 则 $C_G(A) = A$. 若 $A \leqslant Z(G)$, 则 $\Omega_1(G) = A$ 且 $\mho_1(G) \leqslant Z(G)$.*

证明 设 $A = \langle a\rangle \times \langle b\rangle \times \langle c\rangle$. 由定理 14.13.20, 有 $\Omega_1(C_G(A)) = A$.

若 $A \nleqslant Z(G)$, 不妨设 $a \notin Z(G)$. 断言 $C_G(A) = \Omega_1(C_G(A))$: 若否, 则存在 $x \in C_G(A) \setminus \Omega_1(C_G(A))$. 设 $o(x) = p^k$. 则 $k \geqslant 2$ 且 $x^{p^{k-1}} \in \Omega_1(C_G(A)) = A$. 若 $\langle x^{p^{k-1}}\rangle \neq \langle a\rangle$, 则 $\langle a, x^{p^{k-1}}\rangle$ 非循环. 由 G 为 $\mathcal{CAC}$ 群可知, $\langle a, b, c, x\rangle/\langle a, x^{p^{k-1}}\rangle$ 循

环, 矛盾. 若 $\langle x^{p^{k-1}}\rangle=\langle a\rangle$, 则 $\langle a,b,c,x\rangle/\langle a,b\rangle$ 循环, 也得出矛盾. 于是 $C_G(A)=\Omega_1(C_G(A))=A$.

若 $A\not\leqslant Z(G)$, 则 $\Omega_1(G)=\Omega_1(C_G(A))=A$. 任取 $x\in G$. 设 $o(x)=p^k$. 若 $x^p\notin Z(G)$, 则 $k\geqslant 3$. 任取 $y\in A\setminus\langle x^{p^{k-1}}\rangle$. 则 $\langle x^p,y\rangle$ 非循环. 由 G 为 $\mathcal{CAC}$ 群, 故 $\langle a,b,c,x\rangle/\langle x^p,y\rangle$ 循环, 矛盾. 于是 $x^p\in Z(G)$. 因此, 由 x 的任意性, 可得 $\mho_1(G)\leqslant Z(G)$. □

引理 14.13.22 *设 G 是亚循环 p 群, $p>2$. 则 G 是 $\mathcal{CAC}$ 群当且仅当 G 是内交换群.*

证明 设 G 是内交换群, 由定理 1.7.7 可知, $Z(G)=\Phi(G)$. 设 H 为 G 的非循环交换子群且 $H\not\leqslant Z(G)$. 则 $H\not\leqslant\Phi(G)$. 得到 $H\not\leqslant\Phi(C_G(H))$. 由 G 亚循环得 $C_G(H)$ 也亚循环. 从而 $d(C_G(H))\leqslant 2$. 于是存在 $g\in G$ 使得 $C_G(H)=\langle H,g\rangle$. 进而 $C_G(H)/H$ 循环. 因此 G 是 $\mathcal{CAC}$ 群.

反之, 若 G 是亚循环的 $\mathcal{CAC}$ 群, 不妨设 G 如定理 6.1.3 所设. 计算可知, $Z(G)=\langle a^{p^{s+u}},b^{p^{s+u}}\rangle$. 若 $a^p\in Z(G)$, 则 $|G'|=p$. 再由定理 1.7.7 可知, G 内交换. 若 $a^p\notin Z(G)$, 下证这种情形不出现. 若否, 对 $\langle a^p,b^{p^{s+u}}\rangle$ 进行讨论. 若 $\langle a^p,b^{p^{s+u}}\rangle$ 非循环, 则 $\langle a,b^{p^{s+u-1}}\rangle/\langle a^p,b^{p^{s+u}}\rangle$ 循环. 又推出 $\langle a,b^{p^{s+u-1}}\rangle$ 循环, 矛盾. 若 $\langle a^p,b^{p^{s+u}}\rangle$ 循环, 则 $\langle b^{p^{s+u}}\rangle\leqslant\langle a\rangle\bigcap\langle b\rangle=\langle b^{p^{r+s+t}}\rangle$. 这推出 $t=0$, $r=u$. 令 $b_1=ba^{-1}$. 则 $b_1^{p^{r+s}}=1$ 且 $\langle a^{p^{r+s}},b_1^{p^{r+s-1}}\rangle\not\leqslant Z(G)$. 由 G 是 $\mathcal{CAC}$ 群得, $\langle a^p,b_1\rangle/\langle a^{p^{s+r}},b_1^{p^{s+r-1}}\rangle$ 循环. 又由 $\langle a^{p^{s+r}},b_1^{p^{s+r-1}}\rangle\leqslant\Phi(\langle a^p,b_1\rangle)$, 有 $\langle a^p,b_1\rangle$ 循环, 矛盾. 因此 $a^p\notin Z(G)$ 不成立. □

容易看出引理 14.13.22 对通常亚循环 2 群也成立.

引理 14.13.23 *设 G 为 p^n 阶 $\mathcal{CAC}$ 群, $n\geqslant 6$. 则 G 中不存在交换极大子群 M 使得 $r(M)=3$.*

证明 若否, 设 $M\lessdot G$ 且 $M=\langle x\rangle\times\langle y\rangle\times\langle z\rangle$, $o(x)=p^i,o(y)=p^j,o(z)=p^k$, 其中 $i\geqslant 1,j\geqslant 1,k\geqslant 1$. 由引理 14.13.21 知, $\Omega_1(G)=\Omega_1(M)\leqslant Z(G)$ 且 $\mho_1(G)\leqslant Z(G)$. 因为 $M\not\leqslant Z(G)$, 不妨设 $x\notin Z(G)$. 又 G 为 $\mathcal{CAC}$ 群, 故 $\langle x,y,z\rangle/\langle x,y^{p^{j-1}}\rangle$ 循环. 这推出 $j=1$. 同理, $k=1$. 于是 $\langle x^p\rangle\times\langle y\rangle\times\langle z\rangle=Z(G)$ 且 $i\geqslant 3$. 若存在 $a\in G\setminus M$ 使得 $\langle a,x^{p^2}\rangle$ 非循环, 则 $\langle a,x^p,y,z\rangle/\langle a,x^{p^2}\rangle$ 循环, 矛盾. 于是, 任取 $a\in G\setminus M$, 均有 $\langle a,x^{p^2}\rangle$ 循环. 由 $a^p\in Z(G)$ 可知 $o(a)\leqslant o(x)$. 故可设 $x^{p^2}=a^p$ 或 $x^{p^2}=a^{p^2}$. 若 $x^{p^2}=a^p$, 则 $a^{-1}x^p\in\Omega_1(G)\leqslant M$. 从而 $a\in M$, 矛盾. 若 $x^{p^2}=a^{p^2}$, 则由 $[a,x]\in Z(G)$ 可得 $o(ax^{-1})=p^2$. 注意到 $ax^{-1}\notin M$, 由此可知 $x^{p^2}=(ax^{-1})^p$, 进而得到矛盾. □

引理 14.13.24 *设 G 为 p^n 阶 $\mathcal{CAC}$ 群, $n\geqslant 6$ 且 $r(G)=3$. 若 $p>2$, 则 G 中不存在交换极大子群. 若 $p=2$ 且 G 中存在交换极大子群, 则 G 为下列互不同构的群之一.*

(1) $\mathrm{D}_{2^{n-1}}\times \mathrm{C}_2$;

(2) $\mathrm{SD}_{2^{n-1}}\times \mathrm{C}_2$;

(3) $\langle a,b,c \mid a^4=b^2=c^{2^{n-3}}=1,[b,a]=c,[c,a]=[c,b]=c^{-2}\rangle$.

证明　设 G 有交换极大子群 M. 由引理 14.13.23 可知 $r(M)\leqslant 2$. 又由 $r(G)=3$ 得 $r(M)=2$. 设 $M=\langle x\rangle\times\langle y\rangle$, $o(x)=p^i,o(y)=p^j$, 其中 $i\geqslant 1,j\geqslant 1$, $A\leqslant G$ 且 $A\cong \mathrm{C}_p^3$. 因为 $Z(G)\leqslant M$, 故 $A\nleqslant Z(G)$ 且 $G=MA$. 由引理 14.13.21 得 $A=C_G(A)$. 这推出 $Z(G)=M\bigcap A=\Omega_1(M)$. 又 $n\geqslant 6$, 不妨设 $i\geqslant 3$. 从而 $\langle x^p,y^{p^{j-1}}\rangle\nleqslant Z(G)$. 又由 G 为 $\mathcal{CAC}$ 群得, $\langle x,y\rangle/\langle x^p,y^{p^{j-1}}\rangle$ 循环. 推出 $o(x)=p^{n-2},o(y)=p$. 任取 $g\in A\setminus M$. 则 $G=\langle x,y,g\rangle$. 由定理 1.7.6 得 $|G'|=p^{n-3}$. 设 $[x,g]=x^{ps}y^t$. 易知 $G'=\langle x^{ps}y^t\rangle$. 于是 $(s,p)=1$.

若 $p>2$, 由引理 1.11.4 知, G 正则. 从而 $[x,g^p]=1$ 当且仅当 $[x,g]^p=1$. 但是 $[x,g]^p=x^{sp^2}\neq 1$, 矛盾.

若 $p=2$, 由 $[x,g^2]=1$ 可知, $[x,g]=x^{-2}$, 或 $x^{2^{n-3}-2}$, 或 $x^{-2}y$ 或 $x^{2^{n-3}-2}y$. 若 $[x,g]=x^{-2}$, 则 $G\cong \mathrm{D}_{2^{n-1}}\times\mathrm{C}_2$. 若 $[x,g]=x^{2^{n-3}-2}$, 则 $G\cong \mathrm{SD}_{2^{n-1}}\times \mathrm{C}_2$. 若 $[x,g]=x^{-2}y$, 令 $x_1=gx$, $y_1=x^2y$. 则 $G=\langle x_1,g,y_1 \mid x_1^4=g^2=y_1^{2^{n-3}}=1,[g,x_1]=y_1,[y_1,g]=[y_1,x_1]=y_1^{-2}\rangle$. 此时 G 同构于 (3) 型群. 若 $[x,g]=x^{2^{n-3}-2}y$, 则 G 也同构于 (3) 型群. □

引理 14.13.25　*设 G 为 $\mathcal{CAC}$ 群, H 为 G 的非交换子群. 则*

(1) H 为 $\mathcal{CAC}$ 群;

(2) 若 $Z(H)$ 非循环, 则 $Z(H)\leqslant Z(G)$.

证明　(1) 设 K 为H 的任意非循环交换子群且$K\nleqslant Z(H)$, 则 $K\nleqslant Z(G)$. 由 G 是 $\mathcal{CAC}$ 群得 $C_G(K)/K$ 循环. 从而 $C_H(K)/K$ 循环. 于是 H 为 $\mathcal{CAC}$ 群.

(2) 由 $\mathcal{CAC}$ 群的定义可直接得到结论. □

引理 14.13.26　*设 G 是 p 群, 若 $Z(G)$ 循环且 $|G:Z(G)|=p^2$, 则 G 为 $\mathcal{CAC}$ 群.*

证明　设 H 为 G 的任意非循环交换子群且 $H\nleqslant Z(G)$. 则 $C_G(H)<G$ 且 $C_G(H)\geqslant HZ(G)$. 比较阶可知 $C_G(H)=HZ(G)$. 从而 $C_G(H)/H\cong Z(G)/Z(G)\bigcap H$ 循环. 因此 G 为 $\mathcal{CAC}$ 群. □

下面我们仅给出 $\mathcal{CAC}$ 群的分类结果, 证明过程略去.

定理 14.13.27　*设 G 为 p^n 阶群, $n\geqslant 7$ 且 $p>2$. 则 G 为 $\mathcal{CAC}$ 群当且仅当 G 为下列互不同构的群之一.*

(1) 内交换的亚循环群;

(2) $\mathrm{M}_p(1,1,1)*\mathrm{C}_{p^{n-2}}$;

(3) $\langle a,x,y \mid a^{p^{n-2}}=x^p=y^p=1,[a,x]=y,[x,y]=a^{ip^{n-3}},[y,a]=1\rangle$, $i=1$ 或 σ, 这里 σ 是一个固定的模 p 的平方非剩余.

定理 14.13.28 设 G 为 2^n 阶群, 其中 $n \geqslant 6$. 则 G 为 CAC 群当且仅当 G 为下列互不同构的群之一.

(1) 内交换的亚循环群;

(2) 极大类群;

(3) $D_{2^{n-1}} \times C_2$;

(4) $SD_{2^{n-1}} \times C_2$;

(5) $Q_{2^{n-1}} \times C_2$;

(6) $D_8 * C_{2^{n-2}}$;

(7) $\langle a, b \mid a^4 = b^{2^{n-2}} = 1, [b, a] = b^{-2} \rangle$;

(8) $\langle a, b \mid a^4 = b^{2^{n-2}} = 1, [b, a] = b^{2^{n-3}-2} \rangle$;

(9) $\langle a, b \mid a^8 = b^{2^{n-2}} = 1, a^4 = b^{2^{n-3}}, [b, a] = b^{-2} \rangle$;

(10) $\langle a, b, c \mid a^{2^{n-3}} = b^4 = 1, c^2 = a^2b^2, [b, a] = b^2, [c, a] = [c, b] = 1 \rangle$;

(11) $\langle a, b, c \mid a^{2^{n-3}} = b^4 = 1, c^2 = a^2b^2, [b, a] = b^2, [c, a] = a^{2^{n-4}}, [c, b] = 1 \rangle$;

(12) $\langle a, b, c \mid a^4 = b^2 = c^{2^{n-3}} = 1, [b, a] = c, [c, a] = [c, b] = c^{-2} \rangle$;

(13) $\langle a, b, c \mid a^4 = b^4 = c^{2^{n-3}} = 1, b^2 = c^{2^{n-4}}, [b, a] = c, [c, a] = [c, b] = c^{-2} \rangle$;

(14) $\langle a, b, c \mid a^8 = b^2 = c^{2^{n-3}} = 1, a^4 = c^{2^{n-4}}, [b, a] = c, [c, a] = [c, b] = c^{-2} \rangle$;

(15) $\langle a, b, c \mid a^{2^{n-2}} = b^2 = c^4 = 1, c^2 = a^{2^{n-3}}, [b, a] = a^2, [c, a] = [c, b] = 1 \rangle$;

(16) $\langle a, b, c \mid a^{2^{n-2}} = b^2 = c^4 = 1, c^2 = a^{2^{n-3}}, [b, a] = c, [c, b] = c^2, [c, a] = 1 \rangle$;

(17) $\langle a, b, c, d, e \mid a^4 = d^2 = e^2 = 1, a^2 = b^2 = c^2, [b, a] = a^2, [c, a] = d, [c, b] = e, [d, a] = [e, a] = [d, b] = [e, b] = [c, d] = [c, e] = [d, e] = 1 \rangle$;

(18) $\langle a, b, c, d \mid a^4 = b^4 = d^2 = 1, b^2 = c^2, [b, a] = b^2, [c, a] = a^2, [c, b] = d, [d, a] = [d, b] = [c, d] = 1 \rangle$;

(19) $\langle a, b, c, d \mid a^4 = b^4 = d^2 = 1, a^2 = c^2, [b, a] = a^2, [c, a] = b^2c^2, [c, b] = d, [d, a] = [d, b] = [c, d] = 1 \rangle$;

(20) $\langle a, b, c \mid a^4 = b^4 = c^4 = 1, [b, a] = c^2, [c, a] = b^2c^2, [c, b] = a^2b^2 \rangle$;

(21) $\langle a, b, c, d \mid a^4 = b^4 = 1, c^2 = a^2b^2, a^2 = d^2, [a, b] = b^2, [a, c] = a^2, [a, d] = b^2, [b, c] = 1, [b, d] = a^2, [c, d] = c^2 \rangle$.

当 G 为 2^5 阶群时, 验证 2^5 阶群表或使用 Magma 可得所求的 CAC 群. 文献 [221] 列出了结果. 作为练习, 读者可求出这些群.

14.13.3 有一个自中心化循环正规子群的 p 群

众所周知, 有限 p 群的一个经典分类定理是 Burnside 给出的具有一个循环极大子群的有限 p 群的分类. 郝成功等在文献 [80] 分类了具有一个自中心化循环正规子群的非交换 p 群, 等价地说, 分类了具有循环的极大交换正规子群的非交换 p 群. 本节介绍他们的工作.

引理 14.13.29　设 $A=\langle a\rangle$ 为 2^n 阶循环群且 $n\geqslant 3$, $\mathrm{Aut}(A)=\langle\alpha\rangle\times\langle\beta\rangle$, 其中 $a^\alpha=a^{-1}$, $a^\beta=a^5$. 对每个正整数 $m\leqslant n-2$, 定义 $a^{\beta_m}=a^{1+2^{n-m}}$. 则

(1) $\beta_m\in\langle\beta\rangle$, $o(\beta_m)=2^m$. 特别地, $\beta_1=(\beta_m)^{2^{m-1}}$.

(2) $\langle\alpha,\beta_m\rangle$ 是 $\mathrm{Aut}(A)$ 的唯一的 2^{m+1} 阶非循环子群.

证明　(1) 若 $\beta_m\notin\langle\beta\rangle$, 对某个 $i\geqslant 0$, 记 $\beta_m=\alpha\beta^i$. 则 $a^{\alpha\beta^i}=a^{-5^i}=a^{1+2^{n-m}}$. 因而 $-5^i\equiv 1+2^{n-m}\,(\mathrm{mod}\,2^n)$. 由假设 $m\leqslant n-2$ 得 $-5^i\equiv 1\,(\mathrm{mod}\,4)$, 矛盾. 计算可得, $o(\beta_m)=2^m$ 且 $\beta_1=(\beta_m)^{2^{m-1}}$.

(2) 设 Δ 为 $\mathrm{Aut}(A)$ 的一个 2^{m+1} 阶非循环子群. 因为 $\mathrm{Aut}(A)$ 是型为 $(2,2^{n-2})$ 的交换 2 群, 且由 (1) 知 $\langle\beta_m\rangle$ 是含在 $\langle\beta\rangle$ 的唯一的 2^m 阶子群, 由此可得, $\exp(\Delta)=2^m$ 且 $\Delta\subseteq\Omega_m(\mathrm{Aut}(A))=\langle\alpha,\beta_m\rangle$. 比较阶可知 $\Delta=\langle\alpha,\beta_m\rangle$. □

定理 14.13.30　设 P 为有限非循环 p 群. 则 P 有一个极大的交换正规子群为 p^n 阶循环群当且仅当 P 为以下几种互不同构的类型:

(1) $\mathrm{Q}_{2^{n+1}}=\langle a,b\mid a^{2^n}=1,\ b^2=a^{2^{n-1}},\ a^b=a^{-1}\rangle$, 其中 $n\geqslant 2$;

(2) $\mathrm{D}_{2^{n+1}}=\langle a,b\mid a^{2^n}=b^2=1,\ a^b=a^{-1}\rangle$, 其中 $n\geqslant 2$;

(3) $\mathrm{M}_p(n,m)=\langle a,b\mid a^{p^n}=b^{p^m}=1,\ a^b=a^{1+p^{n-m}}\rangle$, 其中 $n>m$, 当 $p=2$ 时 $n\geqslant m+2$;

(4) $S(n,m)=\langle a,b\mid a^{2^n}=b^{2^m}=1,\ a^b=a^{-1-2^{n-m}}\rangle$, 其中 $n\geqslant m+2$;

(5) $M^*(n,m)=\langle a,b,c\mid a^{2^n}=b^{2^m}=c^2=1,\ a^b=a^{1+2^{n-m}},\ a^c=a^{-1+2^{n-1}},\ b^c=b\rangle$, 其中 $n\geqslant m+2$;

(6) $M_*(n,m)=\langle a,b,c\mid a^{2^n}=b^{2^m}=c^2=1,\ a^b=a^{1+2^{n-m}},\ a^c=a^{-1+2^{n-1}},\ b^c=aba^{-1}\rangle$, 其中 $n\geqslant m+2$.

证明　若 P 为定理中的群, 容易验证 P 是非循环的且 $\langle a\rangle$ 为 P 的自中心化的正规子群. 因此 $\langle a\rangle$ 为 P 的极大交换正规子群.

反过来, 设 A 为 P 的一个循环的极大交换正规子群. 令 $A=\langle a\rangle, o(a)=p^n$, 则 $C_P(A)=A$. 由 N/C 定理可知 P/A 同构于 $\mathrm{Aut}(A)$ 的一个子群.

若 p 为奇素数, 熟知 $\mathrm{Aut}(A)\cong U(\mathbb{Z}_{p^n})$ 为 p^{n-1} 阶循环群, 所以 P/A 也是循环群. 令 $|P/A|=p^m$, 则 $m<n$. 定义 $\gamma\in\mathrm{Aut}(A)$ 为 $a^\gamma=a^{1+p^{n-m}}$, 根据引理 12.3.5 可知 γ 为 A 的 p^m 阶自同构, 故 $\langle\gamma\rangle$ 为 $\mathrm{Aut}(A)$ 唯一的 p^m 阶子群. 由此可知, 存在 $b\in P$ 使得 $P/A=\langle bA\rangle$ 并且 $a^b=a^{1+p^{n-m}}$. 设 $b^{p^m}=a^t$. 由定理 6.1.3 可知 $p^m\mid t$. 经过适当的替换后, 我们可不妨设 $b^{p^m}=1$. 从而 $P\cong\mathrm{M}_p(n,m)$.

以下考虑 $p=2$ 的情形. 易知 P/A 为交换群, 设其方次数为 2^m. 再从 P 的非交换性假设推出 $n\geqslant 2$. 以下分两种情形论证:

(1) P/A 为循环群的情形, 此时 $P\cong\mathrm{Q}_{2^{n+1}}$, $\mathrm{D}_{2^{n+1}}$, $M(n,m)$, $S(n,m)$.

如果 $n=2$, 则 $\mathrm{Aut}(A)$ 为 2 阶循环群, 迫使 $|P/A|=2$; 并且从 $|A|=2^2$ 可推出 $|P|=2^3$, 从而 $P\cong\mathrm{Q}_8$ 或 D_8, 结论显然成立. 以下可设 $n\geqslant 3$, 此时 $m\leqslant n-2$.

如果 $m=1$, 则 A 为 P 的循环极大子群, 故归结为经典情形, 熟知 P 同构于下述四类群中的一个群: $\mathrm{Q}_{2^{n+1}}$, $\mathrm{D}_{2^{n+1}}$, $\mathrm{SD}_{2^{n+1}}=S(n,1)$, $M_{2^{n+1}}=\mathrm{M}_2(n,1)$, 结论成立.

再考虑 $m>1$ 的情形. 使用引理 14.13.29 的符号和结论, 可知 $\langle\beta_m\rangle$ 和 $\langle\alpha\beta_m\rangle$ 为 $\mathrm{Aut}(A)$ 的仅有的两个 2^m 阶循环子群. 故而存在 $b\in P$ 使得 $P/A=\langle bA\rangle$, 即 $P=\langle a,b\rangle$, 且 $a^b=a^{1+2^{n-m}}$ 或者 $a^b=a^{-(1+2^{n-m})}$. 设 $b^{2^m}=a^t$. 由定理 6.1.4 可知 $2^m\mid t$. 经过适当的替换后, 我们可不妨设 $b^{2^m}=1$. 从而 $P\cong\mathrm{M}_2(n,m)$ 或 $S(n,m)$, 结论得证.

(2) P/A 为非循环群的情形, 此时 $P\cong M^*(n,m)$, $M_*(n,m)$.

我们仍然使用引理 14.13.29 中的符号和结论. 因为 P/A 同构于 $\mathrm{Aut}(A)$ 唯一的 2^{m+1} 阶非循环子群 $\langle\beta_m\rangle\times\langle\alpha\beta_1\rangle$, 故存在 $b,c\in P$ 使得

$$P/A=\langle bA\rangle\times\langle cA\rangle \text{ 且 } a^b=a^{\beta_m}=a^{1+2^{n-m}},\quad a^c=a^{\alpha\beta_1}=a^{-1-2^{n-1}}=a^{-1+2^{n-1}}.$$

经过适当的替换后, 可不妨设 $b^{2^m}=1$ 和 $o(c)=2$.

令 $M=\langle a,b\rangle=\langle a\rangle\rtimes\langle b\rangle$. 注意到 P/A 为交换群, 故 $[b,c]\in P'\leqslant A$, 表明 c 正规化 M, 即 $M\lhd P$. 此时 $\langle b^c\rangle$ 也是 A 在 M 中的一个补, 因而与 $\langle b\rangle$ 共轭, 故可令 $b^c=a^kb^ia^{-k}$, 其中 i 为奇数且 $k\geqslant 0$. 但 $b^{-1}b^c=[b,c]\in\langle a\rangle$, 迫使 $b^i=b$, 所以 $b^c=a^kba^{-k}$.

如果 $2|k$, 令 $c'=ca^k$, 则 $b^{c'}=b$; 如果 $2\nmid k$, 令 $c'=ca^{k-1}$, 则 $b^c=aba^{-1}$. 此时不难验证总有 $o(c')=2$, 显然还成立 $a^{c'}=a^{-1+2^{n-1}}$. 因为 $\langle c'A\rangle=\langle cA\rangle$, 故可用 c 来替换 c', 根据所给的生成元和关系, 即可推出 $P\cong M^*(n,m)$ 或 $M_*(n,m)$. □

由定理 14.13.30 不难得到下列结论.

引理 14.13.31 设 P 是定理 14.13.30中的群之一, 则下列结论成立.

(a) 若 $P=\mathrm{Q}_{2^{n+1}}$, 则 $P'=\langle a^2\rangle$, $Z(P)=\langle a^{2^{n-1}}\rangle$, $\Omega_1(P)=\langle a^{2^{n-1}}\rangle$.

(b) 若 $P=\mathrm{D}_{2^{n+1}}$, 则 $P'=\langle a^2\rangle$, $Z(P)=\langle a^{2^{n-1}}\rangle$, $\Omega_1(P)=D_{2^{n+1}}$.

(c) 若 $P=\mathrm{M}_p(n,m)$, 则 $P'=\langle a^{p^{n-m}}\rangle$, $Z(P)=\langle a^{p^m}\rangle$, $\Omega_1(P)=\langle a^{p^{n-1}},b^{p^{m-1}}\rangle$, $\Omega_m(P)=\langle a^{p^{n-m}},b\rangle$.

(d) 若 $P=S(n,m)$, 则 $P'=\langle a^2\rangle$, $Z(P)=\langle a^{2^{n-1}}\rangle$, $\Omega_m(P)=\langle a^2,b\rangle$, 而对 $m>1$ 有 $\Omega_1(P)=\langle a^{2^{n-1}},b^{2^{m-1}}\rangle$.

(e) 若 $P=M^*(n,m)$, 则 $P'=\langle a^2\rangle$, $Z(P)=\langle a^{2^{n-1}}\rangle$, $\Omega_1(P)=\langle a,b^{2^{m-1}},c\rangle$.

(f) 若 $P=M_*(n,m)$, 则 $P'=\langle a^2\rangle$, $Z(P)=\langle a^{2^{n-1}}\rangle$, $\Omega_1(P)=\langle a^2,b^{2^{m-1}},c\rangle$.

特别地, 对于 $p=2$, $Z(P)=2$, 除非 $P\cong\mathrm{M}_2(n,m)$.

由引理 14.13.31 不难证明定理 14.13.30 中的群互不同构.

推论 14.13.32 设 P 是有限 2 群, 它有一个自中心化的循环正规子群. 则 P 的自同构群也是 2 群, 除非 $P\cong\mathrm{Q}_8$.

证明 众所周知, 当 $P = \mathrm{Q}_{2^{n+1}}$ 或 $\mathrm{D}_{2^{n+1}}$ 时, 结论成立. 对于其他情形, 通过构造特征子群列

$$1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_s = P,$$

在不同情形下证明: 对每个 i, N_i/N_{i-1} 的自同构群还是 2 群. 由 [69] 中的定理 5.3.2 可知, P 的自同构群也是 2 群.

情形 1 $P = \mathrm{M}_2(n, m)$ 或 $S(n, m)$.

考虑 P 的特征子群列

$$1 \subseteq P' \subseteq \Omega_m(P) \subseteq P.$$

由引理 14.13.31 可知, 上述群列中每个商因子的自同构群是循环的. 从而是 2 群.

情形 2 $P = M^*(n, m)$.

由引理 14.13.31 和定理 14.13.30 可知

$$C_P(P') = C_P(a^2) = \langle a, b^{2^{m-1}} \rangle \cong \mathrm{M}_2(n, 1).$$

由情形 1 可知, $C_P(P')$ 的自同构群是 2 群. 考虑 P 的特征子群列

$$1 \subseteq C_P(P') \subseteq \Omega_1(P) \subseteq P.$$

再一次由引理 14.13.31 可知, 除了 $C_P(P')$ 之外, 上述群列中每个商因子的自同构群是循环的. 从而是 2 群.

情形 3 $P = M_*(n, m)$.

计算易得 $C_P(P') = \langle a, b^{2^{m-1}} \rangle \cong \mathrm{M}_2(n, 1)$. 由情形 1 的论证可知, 它的自同构群是 2 群. 又由引理 14.13.31 可知,

$$C_P(P')\Omega_1(P) = \langle a, b^{2^{m-1}}, c \rangle.$$

通过构造特征子群列

$$1 \subseteq C_P(P') \subseteq C_P(P')\Omega_1(P) \subseteq P,$$

情形 2 的论证意味着 $\mathrm{Aut}(P)$ 是 2 群. □

作为定理 14.13.30 的应用, 下面的定理 14.13.33 推广了 Wong 的一个定理 (见 [193] 中的 10.2.2). 而定理 14.13.34 给出了定理 14.13.30 中群的的特征标刻画. 证明略去.

定理 14.13.33 设 G 是有限群, P 是 G 的 Sylow 2 子群且 P 有一个极大正规交换子群是循环的. 则

(a) 若 $|Z(P)| > 2$, 则 G 有正规子群 N 使得 G/N 是阶为 $|Z(P)|$ 的循环群;

(b) 若 $P' < Z(P)$, 则 G 是 2 幂零的.

特别地, 在上述两种情形下, G 不是单群.

定理 14.13.34 设 P 是非循环的 p 群. 则下列陈述等价.

(a) P 有一个循环正规子群 N, 且 N 有一个不可约复特征标 φ 满足 $\varphi^P \in \mathrm{Irr}(P)$;

(b) 对于 P 的某个循环正规子群 A, P 有一个次数为 $|P:A|$ 的不可约复特征标;

(c) P 同构于定理 14.13.30 中的群之一.

14.14 两个共轭元生成小阶子群的 p 群

本节内容取自文献 [142]. 吕恒等在该文中研究了两个共轭元生成小阶子群的 p 群. 他们如下定义这样的群: 设 G 是有限 p 群. 若对任意 $x, y \in G$ 都有 $|\langle x, x^y\rangle : \langle x\rangle| \leqslant p$, 则称 G 是 K_1 群 (或 $G \in K_1$); 若对任意 $x \in G$ 和 $H \leqslant G$ 都有 $|\langle H, H^x\rangle : H| \leqslant p$, 则称 G 是 K_2 群 (或 $G \in K_2$). 显然 K_1 的子群和商群都是 K_1 群. K_2 群是 K_1 群, 但 K_1 群不一定是 K_2 群, 后面的例子 14.14.7 将说明这个事实.

K_1 群与 J 群和 $\mathrm{BI}(p)$ 群由密切联系. J 群和 $\mathrm{BI}(p)$ 群的定义可参看 11.7 节. 显然, 一个 $\mathrm{BI}(p)$ 群一定是 J 群, 但例 11.7.1 表明, 存在 2 群 $G \in J$ 但 $G \notin \mathrm{BI}(2)$. 然而, 当 $p \geqslant 3$ 时, J 群与 $\mathrm{BI}(p)$ 群是同一类群, 参看命题 11.7.2. 我们还可找到一个 K_2 群, 但不是 $\mathrm{BI}(p)$ 群. 例如, $H = \langle a, b_1, b_2, \cdots, b_m\rangle$, 其中

$$a^p = b_1^{p^2} = \cdots = b_n^{p^2} = 1, \quad [b_i, a] = b_i^p, \quad [b_i, b_j] = 1, \quad 1 \leqslant i, j \leqslant n.$$

则 $H \in K_2$ 但 $H \notin \mathrm{BI}(p)$. 因此 K_1 群与 $\mathrm{BI}(p)$ 群和 J 群是不同的群类.

设 $G \in K_1$, $x \in G$ 是 p 阶元. 则对任意 $g \in G$ 有 $|\langle x, x^g\rangle| \leqslant p^2$ 且 $[x, x^g] = 1$. 因此有如下引理.

引理 14.14.1 设 $G \in K_1$, $x \in G$ 是 p 阶元. 则 $\langle x\rangle^G$ 是 G 的初等交换子群.

引理 14.14.2 设 $G = \langle x, y\rangle \in K_1$, 其中 $|x| = |y| = p$. 则 $|G| \leqslant p^3$.

证明 由引理 14.14.1 可知 $\langle x^G\rangle$ 和 $\langle y\rangle^G$ 是 G 的初等交换子群. 又 $G = \langle x\rangle^G\langle y\rangle^G$, 由此可得 $c(G) \leqslant 2$. 从而得 $|G| \leqslant p^3$. □

引理 14.14.3 设 $G = \langle x, y\rangle \in K_1$ 且 $\langle x\rangle \bigcap \langle y\rangle = 1$. 则 $c(G) \leqslant 3$ 且 G' 是阶不超过 p^3 的初等交换子群. 进一步, 若 $p = 2$, 则 $\mho_2(G) \leqslant Z(G)$; 若 $p \geqslant 3$, 则 $\mho_1(G) \leqslant Z(G)$.

证明　因为 $G \in K_1$, 故对 $g \in G$ 有 $|\langle x, x^g\rangle : \langle x\rangle| \leqslant p$ 成立. 因此 $(\langle x^p\rangle)^g \leqslant \langle x\rangle$ 且 $\langle x^p\rangle^g = \langle x^p\rangle$. 由此表明 $\langle x^p\rangle \trianglelefteq G$. 同理可得 $\langle y^p\rangle \trianglelefteq G$.

令 $N = \langle x^p, y^p\rangle$. 由引理 14.14.2 知 $|G/N| \leqslant p^3$. 于是可得 $|\langle xN\rangle^{G/N}| \leqslant p^2$. 因此

$$|\langle x\rangle^G N : N| \leqslant p^2, \quad |\langle x\rangle^G| \leqslant p^2 |\langle x\rangle^G \bigcap N| = p^2 |\langle x^p\rangle(\langle x\rangle^G \bigcap \langle y^p\rangle)|.$$

令 $\overline{G} = G/\langle x^p\rangle$. 由引理 14.14.1 可知, $\langle \bar{x}\rangle^{\overline{G}}$ 是初等交换群. 又因为 $\langle x\rangle \bigcap \langle y\rangle = 1$, 所以 $|\langle x\rangle^G \bigcap \langle y\rangle| \leqslant p$. 又

$$|\langle x\rangle^G| \leqslant p^2 |\langle x^p\rangle(\langle x\rangle^G \bigcap \langle y^p\rangle)| \leqslant p^3 |\langle x^p\rangle|,$$

因此, $|\langle x\rangle^G : \langle x\rangle| \leqslant p^2$. 进而, 若 $|\langle x\rangle^G : \langle x\rangle| = p^2$, 则 $|\langle x\rangle^G \bigcap \langle y\rangle| = p$. 同理可得 $|\langle y\rangle^G : \langle y\rangle| \leqslant p^2$, 且当 $|\langle y\rangle^G : \langle y\rangle| = p^2$ 时, 可得 $|\langle y\rangle^G \bigcap \langle x\rangle| = p$.

令 $M = \langle x\rangle^G \bigcap \langle y\rangle^G$. 则

$$|M| = |M : \langle x\rangle^G \bigcap \langle y\rangle||\langle x\rangle^G \bigcap \langle y\rangle| \leqslant |\langle y\rangle^G : \langle y\rangle||\langle x\rangle^G \bigcap \langle y\rangle| \leqslant p^3.$$

显然, $|M| = p^3$ 当且仅当 $\Omega_1(\langle x\rangle) \leqslant M$ 且 $\Omega_1(\langle y\rangle) \leqslant M$. 由于 $G/\langle x\rangle^G$ 和 $G/\langle y\rangle^G$ 都是循环群, 因此 G/M 是交换群. 这表明 $G' \leqslant M$. 因此 $|G'| \leqslant p^3$. 若 $|G'| \leqslant p^2$, 则 $c(G) \leqslant 3$. 若 $|G'| = p^3$, 则 $G' = M$. 由 $\Omega_1(\langle x\rangle) \leqslant G'$ 与 $\Omega_1(\langle y\rangle) \leqslant G'$ 可知 $|x| \geqslant p^2$ 且 $|y| \geqslant p^2$. 又 $\langle x^p\rangle \trianglelefteq G$ 且 $\langle y^p\rangle \trianglelefteq G$. 因此 $\Omega_1(\langle x\rangle) \bigcup \Omega_1(\langle y\rangle) \subseteq Z(G)$. 于是 $c(G) \leqslant 3$.

现在证明 G' 是交换群. 对 $a \in G'$, 仅需证明 $a^p = 1$. 因为 $\langle x\rangle \bigcap \langle y\rangle = 1$, 故 $\langle a\rangle \bigcap \langle x\rangle = 1$ 或 $\langle a\rangle \bigcap \langle y\rangle = 1$. 不妨设 $\langle a\rangle \bigcap \langle x\rangle = 1$. 首先考虑 $|G'| \leqslant p^2$ 这种情况. 此时, $|G_3(G)| \leqslant p$. 由于 $G = \langle x, y\rangle$, 故 $a = [x, y]^i z$, 其中 $z \in G_3(G) \leqslant Z(G)$. 因此 $a^p = [x, y]^{ip}$ 且 $a^p \in (\langle x\rangle^G)^p$. 由于 $\langle \bar{x}\rangle^{\overline{G}}$ 是交换群且 $a^p \in \langle x^p\rangle$. 于是由 $\langle a\rangle \bigcap \langle x\rangle = 1$ 可得 $a^p = 1$. 其次设 $|G'| = p^3$. 同上, 仅需考虑 $|x| > p$ 且 $\Omega_1(\langle x\rangle) \leqslant M = G'$ 这种情形. 令 $\tilde{G} = G/\Omega_1(\langle x\rangle)$. 则 $|\tilde{G}| = p^2$. 利用前面结论可得 $\tilde{a}^p = 1$ 且 $a^p \in \langle x\rangle$. 又因为 $\langle x\rangle \bigcap \langle a\rangle = 1$, 故 $a^p = 1$.

由命题 1.1.9 知, 若 $p \geqslant 3$, 则 $[x^p, y] = \prod\limits_{i=1}^{p} [ix, y]^{\binom{p}{i}}$ 且 $x^p \in Z(G)$. 同理 $y^p \in Z(G)$. 若 $p = 2$, 则 $[x^4, y] = \prod\limits_{i=1}^{4} [ix, y]^{\binom{4}{2}}$ 且 $x^4 \in Z(G)$. 同理也可得 $y^4 \in Z(G)$. 令 $g = x^m y^n \in G$. 若 $p \geqslant 3$, 由 Hall-Petrescu 恒等式得

$$(x^m y^n)^p = x^{mp} y^{np} c_2^{\binom{p}{2}} c_3^{\binom{p}{3}} = x^{mp} y^{np} c_3^{\binom{p}{3}},$$

其中 $c_2 \in G', c_3 \in G_3$. 此时 G' 是初等交换群且 $c(G) \leqslant 3$. 因此 $g^p \in Z(G)$. 由此说明 $\mho_1(G) \leqslant Z(G)$. 若 $p = 2$, 再次利用 Hall-Petrescu 恒等式可得

$$(x^m y^n)^4 = x^{4m} y^{4n} c_2^{\binom{4}{2}} c_3^{\binom{4}{3}} = x^{4m} y^{4n},$$

其中 $c_2\in G', c_3\in G_3$. 因为 G' 初等交换群且 $c(G)\leqslant 3$, 所以 $g^4\in Z(G)$ 且 $\mho_2(G)\leqslant Z(G)$. □

定理 14.14.4 *设 G 是 K_1 群. 则下列结论成立.*

(1) 若 $p\geqslant 3$, 则 $\mho_1(G)\leqslant Z(G)$ 且 $\exp(G')=p$. 特别地, 若 $p=3$, 则 $c(G)\leqslant 4$; 若 $p\geqslant 5$, 则 $c(G)\leqslant 3$.

(2) 若 $p=2$, 则 $\mho_2(G)\leqslant Z(G)$, $\exp(G')\leqslant 4$ 且 $c(G)\leqslant 3$.

证明 取 $x,y\in G$, 令 $H=\langle x,y\rangle$. 不妨设 $|x|=p^m\geqslant |y|=p^n$. 因为 $|\langle x,x^y\rangle:\langle x\rangle|\leqslant p$, 所以 $\langle x^p\rangle^y=\langle x^p\rangle$. 于是可得 $\langle x^p\rangle\trianglelefteq G$. 同理 $\langle y^p\rangle\trianglelefteq G$.

(1) 若 $p\geqslant 3$. 我们将证明 $\mho_1(H)\leqslant Z(H)$ 且 H' 初等交换群. 若 $\langle x\rangle\bigcap\langle y\rangle=1$, 由引理 14.14.3 可得 $\mho_1(H)\leqslant Z(H)$ 且 H' 是初等交换群. 因此可设 $\langle x\rangle\bigcap\langle y\rangle\neq 1$.

若 $m\leqslant 2$, 显然 $n\leqslant 2$. 由 $\langle x\rangle\bigcap\langle y\rangle\neq 1$, 下面仅需要考虑 $m=n=2$ 这种情况. 易得 $\langle x^p\rangle=\langle y^p\rangle\trianglelefteq G$. 此时 $\langle x^p\rangle\leqslant Z(H)$ 且 $\langle y^p\rangle\leqslant Z(H)$. 令 $\overline{H}=H/\langle x^p\rangle$. 由引理 14.14.2, $|\overline{H}|\leqslant p^3$, 且 $|\overline{H}'|\leqslant p$, 从而说明 $\overline{H}$ 是正则的. 因此, $\mho_1(\overline{H})=1$ 且 $\mho_1(H)\leqslant\langle x^p\rangle\leqslant Z(H)$. 又因为 $|H'|\leqslant p^2$, 所以 H' 是交换群. 再由命题 1.1.9 可得 $[x,y]^p=1$, 且 H' 是交换群.

若 $m\geqslant 3$. 如果存在元 $y_1\in H$ 使得 $H=\langle x,y_1\rangle$ 且 $\langle x\rangle\bigcap\langle y_1\rangle=1$, 则同上可得结论成立. 下面对 n 归纳证明这样的 y 是存在的. 首先假设 $m>n$. 令 $H_1=\langle x^{p^{m-n}},y\rangle$. 此时 $\langle x^{p^{m-n}}\rangle\trianglelefteq H$. 因此 H_1 是正则的. 于是存在正整数 s 使得 $|x^{sp^{m-n}}y|<|y|$. 由于 $H=\langle x,x^{sp^{m-n}}y\rangle$, 由归纳法得, 存在 $y_1\in H$ 满足条件. 其次假设 $m=n$. 令 $\langle x\rangle\bigcap\langle y\rangle=\langle y^{p^k}\rangle$, 其中 $k\geqslant 1$. 若 $k=1$, 由引理 14.14.2 可得 $|H/\langle y^p\rangle|\leqslant p^3$. 进而可得 $|\langle x\rangle^H:\langle x\rangle|\leqslant p$ 且 $|\langle y\rangle^H:\langle y\rangle|\leqslant p$. 容易得到存在正整数 s 使得 $|x^sy|<p^m$. 又 $H=\langle x,x^sy\rangle$, 再次由归纳法可得 $y_1\in H$ 满足条件. 若 $k\geqslant 2$, 令 $\overline{H}=H/\langle y^{p^{k+1}}\rangle$. 由引理 14.14.3 可得 $(\overline{H}/\langle\bar{y}^{p^k}\rangle)'$ 是阶不超过 p^3 的初等交换群且 $c(\overline{H}/\langle\bar{y}^{p^k}\rangle)\leqslant 3$. 于是 $c(\overline{H})\leqslant 4$, $|\overline{H}'|\leqslant p^4$ 且满足 $|\overline{H}':\Omega_1(\overline{H}')|\leqslant p$. 假设 $\bar{x}^{-sp^k}=\bar{y}^{p^k}$. 由 Hall-Petrescu 恒等式得

$$(\bar{x}^s\bar{y})^{p^k}=\bar{x}^{sp^k}\bar{y}^{p^k}c_2^{\binom{p^k}{2}}c_3^{\binom{p^k}{3}}c_4^{\binom{p^k}{4}}=\bar{x}^{sp^k}\bar{y}^{p^k}=1,$$

其中 $c_i\in G_i(\bar{H}), i=2,3,4$. 则 $|\bar{x}^s\bar{y}|\leqslant p^k$. 因此可得 $|x^sy|<p^n$ 且 $H=\langle x,x^sy\rangle$. 再由归纳法, 又可以找到 $y_1\in G$ 使得 $H=\langle x,y_1\rangle$ 且 $\langle x\rangle\bigcap\langle y_1\rangle=1$. 因此对任意元 $x,y\in G$ 有 $[x^p,y]=1$ 成立. 这表明 $\mho_1(G)\leqslant Z(G)$. 又令 $\overline{G}=G/\mho_1(G)$. 引理 14.14.2 表明 $\overline{G}$ 是 2-Engel 群. 由 [247] 中的定理 3.3.2 可知, 若 $p\geqslant 5$, 则 $c(\overline{G})\leqslant 2$. 于是 $c(G)\leqslant 3$; 若 $p=3$, 则 $c(\overline{G})\leqslant 3$. 于是 $c(G)\leqslant 4$. 注意到对任意 $x,y\in G$ 都有 $[x,y]^p=1$. 再由引理 14.14.2 可得 $\exp(G')=p$.

(2) 若 $p=2$. 我们将证明 $\mho_2(H)\in Z(H)$, 并由此可得 $\mho_2(G)\in Z(G)$. 若 $\langle x\rangle\bigcap\langle y\rangle=1$, 由引理 14.14.3 得, $\mho_2(H)\leqslant Z(H)$ 且 H' 是初等交换. 现在假设

$\langle x\rangle\bigcap\langle y\rangle\neq 1$.

如果 $m=n$ 且 $\langle x\rangle\bigcap\langle y\rangle=\langle x^2\rangle$, 由引理 14.14.2 可得 $|H/\langle x^2\rangle|\leqslant 2^3$, 进而 $\mho_2(H)\leqslant Z(H)$.

若 $m=n$ 且 $\langle x\rangle\bigcap\langle y\rangle=\langle x^4\rangle$, 考虑 $\overline{H}=H/\langle x^4\rangle$. 则由引理 14.14.3 的证明可得 $|\overline{H}|\leqslant 2^5$. 由于 $\overline{H}$ 不是极大类 2 群. 因此有 $|\overline{H}'|\leqslant 4$. 再由引理 14.14.3 得, $\bar{H}'$ 是初等交换群. 于是可得 $\exp(\overline{H})\leqslant 4$ 且 $\mho_2(H)\leqslant\langle x^4\rangle\leqslant Z(H)$.

若 $m=n$ 且 $\langle x\rangle\bigcap\langle y\rangle=\langle x^{2^k}\rangle$, 其中 $k\geqslant 3$. 由引理 14.14.3, $(H/\langle x^{2^k}\rangle)'$ 知, 是阶不超过 2^3 的初等交换群且 $c(H/\langle x^{2^k}\rangle)\leqslant 3$. 于是可得 $|(H/\langle x^{2^{k+1}}\rangle)'|\leqslant 2^4$ 且 $c(H/\langle x^{2^{k+1}}\rangle)\leqslant 4$. 令 $\overline{H}=H/\langle x^{2^{k+1}}\rangle$. 容易得到 $\exp(\overline{H}')\leqslant 4$. 由 Hall-Petrescu 恒等式得

$$(\bar{x}\bar{y})^{2^k}=\bar{x}^{2^k}\bar{y}^{2^k}c_2^{\binom{2^k}{2}}c_3^{\binom{2^k}{3}}c_4^{\binom{2^k}{4}}=\bar{x}^{2^k}\bar{y}^{2^k}=1,$$

其中 $c_i\in K_i(\overline{H})$, $i=2,3,4$. 则 $|\bar{x}\bar{y}|\leqslant 2^k$. 因此 $|xy|<2^m$ 且 $H=\langle x,xy\rangle$.

因此下面仅需要考虑子群 $H=\langle x,y\rangle$, 其中 $|x|=2^m>|y|=2^n$ 且 $\langle x\rangle\bigcap\langle y\rangle\neq 1$. 若 $m\leqslant 3$, 则易得 $\mho_2(H)\leqslant\langle x\rangle\bigcap\langle y\rangle\leqslant Z(H)$.

设 $m\geqslant 4$. 同样我们证明存在 $y_1\in H$ 使得 $H=\langle x,y_1\rangle$ 且 $\langle x\rangle\bigcap\langle y_1\rangle=1$. 下面对 n 归纳.

若 $n=2$, 由引理 14.14.3 知, $(H/\langle y^2\rangle)'$ 是阶不超过 2^3 的初等交换群. 于是可得 $|H'|\leqslant 2^4$ 且 $\exp(H')\leqslant 4$. 此时 $\langle x,x^y\rangle$ 循环或 $\langle x,x^y\rangle\cong \mathrm{M}_{2^{m+1}}$. 若 $\langle x,x^y\rangle$, 则 $\langle x\rangle\trianglelefteq H$. 因为 $m\geqslant 4$ 且 H 是 K_1 群, 所以 $\langle x^{2^{m-2}},y\rangle$ 是交换群, 从而可得 $x^{2^{m-2}}y$ 是 2 阶元. 若 $\langle x,x^y\rangle\cong\mathrm{M}_{2^{m+1}}$, 则 $\langle x,x^y\rangle'$ 是 2 阶循环群. 于是可得

$$[x,y]^2=(x^{-1}x^y)^2=x^{-2}(x^2)^yc_2,$$

其中 $c_2\in\langle x,x^y\rangle'$. 进而得到

$$1=[x,y]^4=(x^{-2}(x^2)^yc_2)^2=[x^2,y]^2c_2^2=[x^2,y]^2.$$

因此 $|\langle x^2,y\rangle'|\leqslant 2$. 且可得 $[x^{2^{m-2}},y]=1$. 这说明 $x^{2^{m-2}}y$ 的阶是 2. 显然, $H=\langle x,x^{2^{m-2}}y\rangle$.

若 $n\geqslant 3$, 令 $\langle x\rangle\bigcap\langle y\rangle=\langle y^{2^k}\rangle$. 假设 $k\geqslant 2$. 考虑 $\overline{H}=H/\langle y^{2^{k+1}}\rangle$. 则 $|\bar{x}|=2^{m-n+k+1}\geqslant 2^4$ 且 $|\bar{y}|=2^{k+1}$. 因此可得 $\exp(\overline{H}')\leqslant 4$. 于是 $[\bar{x},\bar{y}]^4=(\bar{x}^{-1}\bar{x}^{\bar{y}})^4=1$. 此时 $|\langle\bar{x},\bar{x}^{\bar{y}}\rangle:\langle\bar{x}\rangle|\leqslant 2$. 如果 $\langle\bar{x},\bar{x}^{\bar{y}}\rangle$ 是极大类 2 群, 则 $\exp(\langle\bar{x},\bar{x}^{\bar{y}}\rangle')\geqslant 2^3$, 与 $\exp(\bar{H}')\leqslant 4$ 相矛盾. 因此 $\langle\bar{x},\bar{x}^{\bar{y}}\rangle$ 是交换群或 $\langle\bar{x},\bar{x}^{\bar{y}}\rangle\cong\mathrm{M}_{2^{m-n+k+2}}$. 进一步可得 $(\bar{x}^{-1}\bar{x}^{\bar{y}})^4=\bar{x}^{-4}(\bar{x}^4)^{\bar{y}}=1$. 由此可得 $\bar{x}^4\in Z(\bar{H})$. 因为 $\langle\bar{x}^2\rangle\trianglelefteq\overline{H}$, 所以 $c(\langle\bar{x}^2,\bar{y}\rangle)\leqslant 2$ 且 $[\bar{x}^2,\bar{y}]^2=1$, 此时说明 $(\bar{x}^{2^{m-n}}\bar{y})^{2^k}=\bar{x}^{2^{m-n+k}}\bar{y}^{2^k}=1$. 因此 $|\bar{x}^{2^{m-n}}\bar{y}|\leqslant 2^k$ 且 $|x^{2^{m-n}}y|<2^n$. 若 $k=1$, 由于 $\langle x^{2^{m-n}}\rangle\trianglelefteq H$, 则 $\langle x^{2^{m-n}},y\rangle$ 有一个指数是 2 的

循环群. 因为 $n \geqslant 3$, 所以 $\langle x^{2^{m-n}}, y\rangle$ 是交换群或 $\langle x^{2^{m-n}}, y\rangle \cong \mathrm{M}_{2^{n+1}}$, 从而说明 $|x^{2^{m-n}}y| < 2^n$. 显然 $H = \langle x, x^{2^{m-n}}y\rangle$. 故由归纳法, 存在一个元 $y_1 \in H$ 使得 $H = \langle x, y_1\rangle$ 且 $\langle x\rangle \bigcap \langle y_1\rangle = 1$. 由引理 14.14.3 可得 $\mho_2(H) \leqslant Z(H)$.

因此上述情况都表明 $\mho_2(H) \leqslant Z(H)$. 故有 $\mho_2(G) \leqslant Z(G)$. 若 $\exp(G) \leqslant 4$, 由于对任意 $x \in G$ 有 $\langle x^2\rangle \trianglelefteq G$, 故 $\mho_1(H) \leqslant Z(G)$. 于是可得 $c(G) \leqslant 2$. 又因为 K_1 群的商群也是 K_1 群, 所以 $c(G/G^4) \leqslant 2$. 由于 $\mho_2(G) \leqslant Z(G)$, 从而可得 $c(G) \leqslant 3$.

取 $x, y \in G$ 且满足 $|x| = 2^m$. 由于 $\langle x^2\rangle \trianglelefteq G$ 且 $x^4 \in Z(G)$. 则 $(x^2)^y = x^{2+k2^{m-1}}$. 由此可得 $x^{-2}(x^2)^y = x^{k2^{m-1}} \in Z(G)$. 令 $M_1 = \langle x, x^y\rangle$. 由 $|M_1 : \langle x\rangle| \leqslant 2$ 可得 $|M_1'| \leqslant 2$. 再利用 Hall-Petrescu 恒等式可得

$$[x, y]^2 = (x^{-1}x^y)^2 = x^{-2}(x^2)^y c_2,$$

其中 $c_2 \in M_1'$. 因此 $[x, y]^4 = (x^{-2}(x^2)^y c_2)^2 = (x^{k2^{m-1}}c_2)^2 = 1$.

设 $a = [x_1, y_1] \in G'$ 和 $b = [x_2, y_2] \in G'$. 则 $a^4 = b^4 = 1$. 令 $T = \langle a, b\rangle$. 若 $\langle a\rangle \bigcap \langle b\rangle = 1$, 由引理 14.14.3, 可得 $\exp(T) \leqslant 4$. 若 $|a| = |b| = 4$ 且 $\langle a\rangle \bigcap \langle b\rangle = \langle a^2\rangle$, 由引理 14.14.2 可得 $|T/\langle a^2\rangle| \leqslant 2^3$. 因此 $|T| \leqslant 2^4$. 假设 $|T| = 2^4$ 且 $\exp(T) = 2^3$, 则 $T \cong \mathrm{Q}_{2^4}$. 此时由于 $c(G) \leqslant 3$, 则 $T' \leqslant G_3 \leqslant Z(G)$, 与 $T \cong \mathrm{Q}_{2^4}$ 相矛盾. 故可得 $\exp(G') \leqslant 4$. □

下面讨论 K_2 群. 首先不加证明地给出下面的一个引理.

引理 14.14.5 *设 $G = \langle x, y, z\rangle$ 是 p^5 阶群. 则存在元 $x_1, y_1, z_1 \in G$ 使得 $G = \langle x_1, y_1, z_1\rangle$ 且 $[y_1, z_1] = 1$.*

引理 14.14.6 *设 $G \in K_2$ 且 $\exp(G) = p$. 则 $|G'| \leqslant p$.*

证明 若 $p = 2$, 结论显然成立. 下面假设 $p \geqslant 3$.

若存在 $x \in G$ 使得 $|\langle x\rangle^G : \langle x\rangle| = p^2$, 则 $|\langle x\rangle^G| = p^3$. 此时 $|x| = p$. 由引理 14.14.1 和引理 14.14.2 可知, $\langle x\rangle^G$ 是初等交换群, 并且存在 $y, z \in G$ 使得

$$\langle x\rangle^G = \langle x\rangle^{\langle y, z\rangle} = \langle x\rangle \times \langle [x, y]\rangle \times \langle [x, z]\rangle.$$

令 $H = \langle x, y, z\rangle$ 和 $H_1 = \langle y, z\rangle$. 则 $\langle x\rangle^G = \langle x\rangle^H$, 且由引理 14.14.2 可得 $|H_1| \leqslant p^3$. 假设 $H_1 \bigcap \langle x\rangle^G = 1$. 又 $\langle [x, y]\rangle \times \langle [x, z]\rangle \leqslant \langle H_1, H_1^x\rangle$, 因此 $|\langle H_1, H_1^x\rangle : H_1| \geqslant p^2$, 矛盾. 进而可得 $H = \langle x\rangle^H H_1$ 的阶是 p^5. 由引理 14.14.5 可知, 存在 $x_1, y_1, z_1 \in H$ 使得 $H = \langle x_1, y_1, z_1\rangle$ 且 $[y_1, z_1] = 1$. 因为 $H = \langle x_1\rangle^H \langle y_1, z_1\rangle$ 的阶是 p^5, 所以

$$\langle x_1\rangle^H = \langle x_1\rangle^{\langle y_1, z_1\rangle} = \langle x_1\rangle \times \langle [x_1, y_1]\rangle \times \langle [x_1, z_1]\rangle.$$

同理

$$\langle [x_1, y_1]\rangle \times \langle [x_1, z_1]\rangle \leqslant \langle y_1, z_1, y_1^x, z_1^x\rangle.$$

于是可得 $|\langle y_1, z_1, y_1^x, z_1^x\rangle : \langle y_1, z_1\rangle| \geqslant p^2$, 矛盾. 又因为 G 的商群也是 K_2 群, 所以对任意 $x \in G$ 有 $|\langle x\rangle^G : \langle x\rangle| \leqslant p$ 成立. 从而可得 $c(G) \leqslant 2$.

假设 $|G'| \geqslant p^2$. 因为 $c(G) \leqslant 2$ 且 $\exp(G) = p$, 所以存在 x_1, y_1, x_2, y_2 使得

$$|[x_1, y_1]| = |[x_2, y_2]| = p, \quad \langle [x_1, y_1]\rangle \bigcap \langle [x_2, y_2]\rangle = 1.$$

显然当 $i = 1, 2$ 时都有 $\langle x_1\rangle^G \neq \langle x_i\rangle$ 成立, 即

$$\langle x_i\rangle^G = \langle x_i\rangle \times \langle [x_i, y_i]\rangle, \quad \langle x_1\rangle^G \bigcap \langle x_2\rangle^G = 1.$$

令 $L = \langle x_1, x_2\rangle$. 假设 $[x_1, y_2] \neq 1$. 显然有 $\langle y_2\rangle^G \neq \langle y_2\rangle$ 成立. 因此

$$\langle y_2\rangle^G = \langle y_2\rangle \times \langle [x_1, y_2]\rangle, \quad \langle y_2\rangle^G = \langle y_2\rangle \langle [x_2, y_2]\rangle.$$

由 $c(G) = 2$ 可得 $\langle [x_1, y_2]\rangle = \langle [x_2, y_2]\rangle = Z(G) \bigcap \langle y_2\rangle^G$. 由于 $|[G, \langle x_1\rangle^G]| < |\langle x_1\rangle^G| = p^2$, 因此

$$\langle [x_2, y_2]\rangle = \langle [x_1, y_2]\rangle = [G, \langle x_1\rangle^G] = [G, \langle x_1\rangle].$$

于是 $[x_1, y_1] \in \langle [x_2, y_2]\rangle$. 矛盾. 故得 $[x_1, y_2] = 1$. 同理 $[x_2, y_1] = 1$. 又因为 $c(G) \leqslant 2$, 所以 $[x_1, y_1 y_2] = [x_1, y_1]$ 且 $[x_2, y_1 y_2] = [x_2, y_2]$. 这表明 $\langle x_1\rangle^G \langle x_2\rangle^G \leqslant \langle L, L^{y_1 y_2}\rangle$, 且 $|\langle L, L^{y_1 y_2}\rangle : L| \geqslant p^2$, 矛盾. 故可得 $|G'| \leqslant p$. □

例 14.14.7　令 $G = \langle x_1, x_2, \cdots, x_n\rangle$, 其中 $x_{ij} = [x_i, x_j], x_i^p = [x_i, x_{jk}] = 1, i, j, k = 1, \cdots, n$. 则 $\exp(G) = p$, $G \in K_1$ 且 $|G'| = p^{(n-1)n/2}$. 但由引理 14.14.6可知, $G \notin K_2$.

定理 14.14.8　设 $G \in K_2$. 则 $c(G) \leqslant 3$. 特别地, 若 $p \geqslant 3$, 则 G' 是交换群.

证明　由定理 14.14.4 可知, 仅需假设 $p \geqslant 3$. 由引理 14.14.6 可得, $c(G/\mho_1(G)) \leqslant 2$ 且 $|(G/\mho_1(G))'| \leqslant p$. 再由定理 14.14.4 得, $\mho_1(G) \leqslant Z(G)$ 且 $\exp(G') \leqslant p$. 进而可得 $c(G) \leqslant 3$ 且 G' 是初等交换群. □

14.15　仅有唯一的某型 p^3 阶内交换子群的 p 群

通过具有特定性质的子群个数研究群结构已有许多结果. 20 世纪初, Miller 在文献 [160],[161] 给出的经典结果是: 若有限 p 群 G 有唯一的给定阶的循环子群, 则 G 为循环群或极大类 2 群. 作为另一个极端情形, Berkovich 在其 p 群专著 [26] 中 §10 中, 研究了有唯一的给定阶的非循环子群的 p 群结构. 特别地, 描述了具有唯一的 p^3 阶非循环交换子群的有限 p 群的结构. 赵立博和郭秀云在文献 [283] 则分类了具有唯一的某型 p^3 阶内交换子群的有限 p 群. 他们在文献 [285] 也研究了特定阶的子群都同构且交换的有限 p 群. 该领域的更多结果可见 [27] 中 §52 和 §87. 本节介绍文献 [283] 的工作.

定理 14.15.1 设 G 是 p 群且 $p>2$. 若 G 有且只有一个子群同构于 $\mathrm{M}_p(2,1)$, 则 G 只能是群 $\mathrm{M}_p(2,1)$.

证明 若 $|G|\geqslant p^4$, 且 G 有且只有一个子群同构于 $\mathrm{M}_p(2,1)$, 则这个唯一的子群必包含在 G 的某个 p^4 阶子群中. 另一方面, 由 p^4 阶群的分类 (定理 2.4.2) 可知, 这样的群不存在. 故 $|G|=p^3$. 从而 $G\cong \mathrm{M}_p(2,1)$. □

引理 14.15.2 若 G 是下列三种群之一, 则 G 有且只有一个子群同构于 $\mathrm{M}_p(1,1,1)$.

(Ⅰ) $\langle a,b,c \mid a^{p^n}=b^p=c^p=1,[b,c]=a^{p^{n-1}},[a,b]=[a,c]=1\rangle$, 其中 $n\geqslant 2$.

(Ⅱ) $\langle a,b \mid a^{p^n}=b^p=c^p=1,[b,a]=c,[c,b]=a^{tp^{n-1}},[a,c]=1\rangle$, 其中 $n\geqslant 2$, $t=1$ 或 v, v 是一个固定的模 p 的平方非剩余. 若 $|G|=3^4$, 则 $t=1$.

(Ⅲ) $\langle a,b,c \mid a^9=b^3=c^3=1,[a,b]=c,[c,a]=a^3,[b,c]=1\rangle$.

不同类型的群或者相同类型但不同参数的群互不同构.

证明 设 G 是 (Ⅰ) 型群. 若 $n=2$, 容易验结论成立. 假设 $n=k$ 时, 结论成立. 考虑 $n=k+1$. 经计算知, G 仅有一个极大子群 $M=\langle b,c,a^p\rangle$ 满足 M 同构于群

$$\langle a,b,c|a^{p^k}=b^p=c^p=1,[b,c]=a^{p^{k-1}},[a,c]=[a,b]=1\rangle,$$

其中 $k\geqslant 2$, 且其他的极大子群为交换群或亚循环群. 由归纳假设知, G 有且只有一个子群同构于 $\mathrm{M}_p(1,1,1)$. 于是对于 (Ⅰ) 型群, 结论成立.

设 G 是 (Ⅱ) 型群. 若 $n=2$, 则结论成立. 假设 $n=k$ 时, 结论成立. 考虑 $n=k+1$. 经计算知, G 仅有一个极大子群 $M=\langle b,c,a^p\rangle$ 满足 M 同构 $n=k$ 时的 (Ⅰ) 型群, 且其他的极大子群为交换群或亚循环群. 由归纳假设知, G 有且只有一个子群同构于 $\mathrm{M}_p(1,1,1)$. 于是对于 (Ⅱ) 型群, 结论成立.

对于 (III) 型群, 容易检验结论也成立.

现在证明引理中的群互不同构. 注意到群的阶、幂零类以及极大子群的类型, 只需证明 (Ⅱ) 型群中 $t=1$ 和 $t=v$ 时对应的群不同构即可.

为方便, 设

$$G(1)=\langle a_1,b_1,c_1|a_1^{p^n}=b_1^p=c_1^p=1,[b_1,a_1]=c_1,[c_1,b_1]=a_1^{p^{n-1}},[a_1,c_1]=1\rangle,$$

$$G(v)=\langle a,b,c|a^{p^n}=b^p=c^p=1,[b,a]=c,[c,b]=a^{vp^{n-1}},[a,c]=1\rangle.$$

若 $G(1)\cong G(v)$, 则可设 $a_1=a^{i_1}b^{j_1}c^{k_1}$, $b_1=a^{i_2}b^{j_2}c^{k_2}$. 因 $o(a_1)=p^n$, 且 $o(b_1)=p$, 得 $(i_1,p)=1$ 和 $p|i_2$. 进一步, 由 $b\notin\Phi(G)$ 可知 $(j_2,p)=1$. 因

$$\begin{aligned}
a^{p^{n-1}j_2^2i_1v}&=a^{p^{n-1}j_2v(i_1j_2-i_2j_1)}=[c^{i_1j_2-i_2j_1},a^{i_2}b^{j_2}c^{k_2}]\\
&=[a^{i_2}b^{j_2}c^{k_2},a^{i_1}b^{j_1}c^{k_1},a^{i_2}b^{j_2}c^{k_2}]=a^{p^{n-1}j_2v(i_1j_2-i_2j_1)}\\
&=[c^{i_1j_2-i_2j_1},a^{i_2}b^{j_2}c^{k_2}]=[a^{i_2}b^{j_2}c^{k_2},a^{i_1}b^{j_1}c^{k_1},a^{i_2}b^{j_2}c^{k_2}],
\end{aligned}$$

故 $v \equiv (j_2^{-1})^2 \pmod p$, 与 v 是一个固定的模 p 平方非剩余矛盾. □

引理 14.15.3　设 G 是 p 群且 $|G| \geqslant p^5$. 若 G 有且只有一个子群同构于 $\mathrm{M}_p(1,1,1)$, 则 $Z(G)$ 循环且 $r_n(G)=2$.

证明　设 G 的唯一的同构于 $\mathrm{M}_p(1,1,1)$ 的子群是

$$\langle a,b,c \mid a^p=b^p=c^p=1,[a,b]=c,[a,c]=[b,c]=1\rangle.$$

则 $c \in Z(G)$. 若 $Z(G)$ 非循环, 则存在 $z \in Z(G)$ 满足 $\langle a,c,z\rangle \cong \mathrm{C}_p^3$. 从而 $\langle a,b\rangle \cong \langle az,b\rangle \cong \mathrm{M}_p(1,1,1)$, 矛盾. 因此 $Z(G)$ 循环, 且 $Z(\Omega_1(G))$ 循环.

由 [247] 中的定理 2.2.14 知, 只需证不存在 p^3 阶初等交换的正规子群. 若否, 假设 $\mathrm{C}_p^3 \cong M = \langle a,b,c\rangle \trianglelefteq G$. 由 $Z(\Omega_1(G))$ 循环知, 存在 p 阶元 x 满足 $1<[M,x]<M$. 于是可设 $[a,x]=b,[b,x]=1$. 进而 $\langle a,x\rangle \cong \mathrm{M}_p(1,1,1)$. 当 $p>3$ 时, 存在另外一个子群 $\langle a,cx\rangle \cong \mathrm{M}_p(1,1,1)$, 矛盾. 若 $p=3$ 且 $|G| \geqslant p^5$, 则存在 3^5 阶子群 N 包含 $\langle M,x\rangle$. 但是在 SmallGroups(3^5) 中没有一个群既有同构于 C_p^3 的子群, 同时又有唯一的同构于 $\mathrm{M}_p(1,1,1)$ 的子群. 矛盾. □

由引理 14.15.3, [31] 中的定理 4.1, [247] 中的定理 8.3.6、定理 8.4.2 以及引理 14.15.2 即得如下定理.

定理 14.15.4　设 G 是 p 群, $p>2$ 且 $|G| \geqslant p^4$. 则 G 有且只有一个子群同构于 $\mathrm{M}_p(1,1,1)$ 当且仅当 G 同构于下列群之一.

(Ⅰ) $\langle a,b,c|a^{p^n}=b^p=c^p=1,[b,c]=a^{p^{n-1}},[a,b]=[a,c]=1\rangle$, 其中 $n \geqslant 2$;

(Ⅱ) $\langle a,b|a^{p^n}=b^p=c^p=1,[b,a]=c,[c,b]=a^{tp^{n-1}},[a,c]=1\rangle$, 其中 $n \geqslant 2$, $t=1$ 或 v, v 是一个固定的模 p 平方非剩余;

(Ⅲ) $\langle a,b,c|a^9=b^3=c^3=1,[a,b]=c,[c,a]=a^3,[b,c]=1\rangle$.

下面考虑 G 是 2 群的情况. 若 $|G| \geqslant 2^6$, 且 G 有唯一的子群同构于 D_8, 则 G 必存在 2^5 阶子群包含一个同构于 D_8 的子群. 然而使用 Magma 对 SmallGroups (2^5) 中的群检验可知, 没有这样的群满足此条件. 而利用 Magma 对 SmallGroups (2^4) 中的群检验可知, 只有群 $\langle a,b \mid a^8=b^2=1,[a,b]=a^2\rangle$ 满足此条件. 由此得如下结论.

定理 14.15.5　设 G 是 2 群. 若 G 有且仅有一个子群同构于 D_8, 则 G 是 D_8 或者 $\langle a,b \mid a^8=b^2=1,[a,b]=a^2\rangle$.

当 G 有唯一的子群同构于 Q_8 时, 情况要复杂一些. 若 $|G| \leqslant 2^7$, 借助 Magma 得到结论. 若 $|G|>2^7$, 则由引理 14.15.7— 引理 14.15.10 直接得到结论. 在此列出结论, 证明过程略去.

定理 14.15.6　设 G 为 2 群且 $|G| \geqslant 2^4$. 则 G 有且只有一个子群同构于 Q_8 当且仅当 G 同构于下列互不同构的群之一.

(Ⅰ) $\langle a,b,c \mid a^{2^n}=b^2=c^2=1,[b,c]=a^{2^{n-1}},[c,a]=[b,a]=1\rangle$, 其中 $n \geqslant 2$;

(Ⅱ) $\langle a,b,c \mid a^{2^n}=b^2=c^2=1,[b,a]=ca^{2^{n-2}},[c,a]=1,[c,b]=a^{2^{n-1}}\rangle$, 其中 $n\geqslant 4$;

(Ⅲ) $\langle a,b,c,e \mid a^{2^n}=b^2=c^2=e^2=1,[e,a]=a^2,[b,e]=ca^{2^{n-2}},[c,b]=a^{2^{n-1}},[c,e]=[c,a]=[b,a]=1\rangle$, 其中 $n\geqslant 2$;

(Ⅳ) $\langle a,b \mid a^8=b^2=1,[a,b]=a^2\rangle$;

(Ⅴ) $\langle a,b,c \mid a^8=b^2=c^4=1,c^2=a^4,[b,a]=c,[c,a]=[c,b]=c^2\rangle$.

引理 14.15.7 定理 14.15.6 中的任何群有且只有一个子群同构于 Q_8, 并且不同类型的群或者相同类型但不同参数的群互不同构.

引理 14.15.8 设 G 是有限 2 群, G 有且只有一个子群同构于 Q_8. 若 $G=\langle M,x\rangle$, 其中 $M=\langle a,b,c|a^{2^n}=b^2=c^2=1,[b,c]=a^{2^{n-1}},[c,a]=[b,a]=1\rangle \lessdot G$ $(n\geqslant 4)$, 则有下列情形之一成立.

(1) $[a,x]=1,[b,x]=a^{2^{n-1}i},[c,x]=a^{2^{n-1}j}$ 且 $x^2=a^u$, 其中 i,j,u 都是正整数, 且 $(u,2)=1$;

(2) $[a,x]=1,[b,x]=a^{2^{n-2}j}c,[c,x]=1$ 且 $x^2=a^uc$, 其中 j,u 是正整数, 且 $(u,2)=1$;

(3) $[a,x]=1,[b,x]=a^{2^{n-2}j}c,[c,x]=a^{2^{n-1}}$ 且 $x^2=a^u$, 其中 j,u 是正整数, 且 $(u,2)=1$;

(4) $[a,x]=a^{-2},[b,x]=a^{2^{n-2}j}c,[c,x]=1$ 且 $x^2=1$, 其中 $(j,2)=1$;

(5) $[a,x]=a^{-2},[b,x]=a^{2^{n-2}j}c,[c,x]=a^{2^{n-1}}$ 且 $x^2=a^{2^{n-2}k_1}c$, 其中 $(jk_1,2)=1$ 且 $4|(j-k_1)$;

(6) $[a,x]=1,[b,x]=a^{2^{n-1}j}bc,[c,x]=a^{2^{n-1}k}bc,x^2=a^ub^{j+k+1}c^{j+k+1}$, 其中 j,k,u 都是正整数, 且 $(u,2)=1$;

(7) $[a,x]=a^{-2},[b,x]=[c,x]=a^{2^{n-1}}bc,x^2=a^{2^{n-1}}bc$;

(8) $[a,x]=a^{-2},[b,x]=[c,x]=bc,x^2=bc$;

(9) $[a,x]=a^{-2},[b,x]=a^{2^{n-1}j}bc,[c,x]=a^{2^{n-1}k}bc,x^2=1$, 其中 $[b,x]\neq[c,x]$;

(2′) $[a,x]=1,[c,x]=a^{2^{n-2}j}b,[b,x]=1$ 且 $x^2=a^ub$, 其中 j,u 都是正整数, 且 $(u,2)=1$;

(3′) $[a,x]=1,[c,x]=a^{2^{n-2}j}b,[b,x]=a^{2^{n-1}}$ 且 $x^2=a^u$, 其中 j,u 是正整数, 且 $(u,2)=1$;

(4′) $[a,x]=a^{-2},[c,x]=a^{2^{n-2}j}b,[b,x]=1$ 且 $x^2=1$, 其中 $(j,2)=1$;

(5′) $[a,x]=a^{-2},[c,x]=a^{2^{n-2}j}b,[b,x]=a^{2^{n-1}}$ 且 $x^2=a^{2^{n-2}k_1}b$, 其中 $(jk_1,2)=1$ 且 $4|(j-k_1)$.

更进一步, G 是定理 14.15.6中的(Ⅰ), (Ⅱ) 和(Ⅲ) 型群之一.

引理 14.15.9 设 G 是有限 2 群, 且 G 有且只有一个子群同构于 Q_8. 若 G 有一个极大子群同构于定理 14.15.6 中 $n\geqslant 4$ 时的(Ⅲ) 型群, 则 G 也必为定理

14.15.6中的(III) 型群.

引理 14.15.10 设 G 是有限 2 群. 若 G 有且只有一个子群同构于 Q_8, 则 G 的所有极大子群都不同构于定理 14.15.6 中 $n \geqslant 5$ 时的(II) 型群.

14.16 具有一类可补正规子群的 p 群

回顾一下, 群 G 的子群 H 称为在 G 中**可补**, 若存在 G 的子群 K 使得 $G = HK$ 且 $H \bigcap K = 1$. 特别地, 若 G 的正规子群 H 在 G 中可补, 则称 G 在 H 上**可裂**. 群 G 称为**不可分**的, 若它在 G 的任何非平凡的真正规子群上不可裂. 否则 G 称为**可分**的. 群 G 称为**强可分**的, 若它在 G 的任何非平凡的真正规子群上可裂. 传统上, 强可分群被 Christensen[51] 称为$\boldsymbol{nC}$ **群**. 例如, 参见 [20],[46],[52].

很清楚, 一个群的某类子群有补对群的性质和结构有很大影响. 因而许多学者研究某类子群有补的群. 例如, 文献 [12],[19],[72],[78],[79],[109],[111],[135], [157],[184]. 迄今, 虽然在许多论文中研究子群的可补性对有限群结构的影响, 然而对有限 p 群, 在这方面几乎没有什么结果. 王丽芳等在文献 [229] 开始了这方面的研究, 确切地说, 他们研究了所谓的$\boldsymbol{\mathcal{NC}}$ **群**, 即不含在 Frattini 子群里的非平凡真正规子群均有补的有限 p 群. 他们的工作恰是 Kirtland[114] 所做的相反情形. 本节介绍文献 [229] 的工作.

明显地, 有限群 G 是 nC 群当且仅当 G 是 $\Phi(G) = 1$ 的 $\mathcal{NC}$ 群. 特别地, 若 G 是 p 群且是 nC 群, 则 G 是初等交换的. 因而对 p 群 G 而言, 需要研究的是 $\Phi(G) \neq 1$ 的情形. 以下 $\mathcal{NC}$-p 群意指 G 既是 p 群又是 $\mathcal{NC}$ 群.

易证 $\mathcal{NC}$ 群的商群还是 $\mathcal{NC}$ 群, 然而, $\mathcal{NC}$ 群的子群不一定是 $\mathcal{NC}$ 群.

例 14.16.1 设 $G = \langle a_1, b \mid a_1^3 = b^3 = a_2^3 = a_3^3 = a_4^3 = 1, [a_1, b] = a_2, [a_2, a_1] = a_3, [a_2, b] = a_4, [a_3, a_1] = [a_3, b] = [a_4, a_1] = [a_4, b] = 1\rangle$. 则 G 是 $\mathcal{NC}$ 群但不是极大类群. 进一步地, G 有极大子群不是 $\mathcal{NC}$ 群.

证明 设 $M = \langle b, a_2, a_3, a_4\rangle$. 则 $M \cong \mathrm{M}_p(1,1,1) \times \mathrm{C}_p$ 且 $G = M \rtimes \langle a_1\rangle$. 因为 $|M| = 3^4$, 故 $|G| = 3^5$. 因而 $M \lessdot G$. 明显地, $d(M) = 3$. 由定理 14.16.8 可知, M 不是 $\mathcal{NC}$ 群. 另一方面, $G = \Omega_1(G)$, $G' = \langle a_2, a_3, a_4\rangle = \Phi(G)$ 且 $d(G) = 2$. 于是由定理 14.16.8 可得 G 是 $\mathcal{NC}$ 群. 因为 $G_2 \leqslant Z(G) = \langle a_3, a_4\rangle$, 故 $c(G) = 3$. 故 G 不是极大类的. □

定理 14.16.2 设 G 是 $\mathcal{NC}$-p 群. 则 $G = \Omega_1(G)$ 且 $G' = \Phi(G)$. 特别地, 若 G 非交换, 则 $Z(G) \leqslant \Phi(G)$.

证明 首先可证 $G = \Omega_1(G)$. 若否, 则存在 $M \lessdot G$ 使得 $\Omega_1(G) \leqslant M$. 因为 G 是 $\mathcal{NC}$ 群, M 在 G 中有补, 设其为 H. 因为 $M \lessdot G$, 故 $|G : M| = |H| = p$. 于是 $H \leqslant \Omega_1(G) \leqslant M$. 由此可得 $G = MH = M$. 矛盾. 因而 $G = \Omega_1(G)$. 由于

$\overline{G}=G/G'$ 是 $\mathcal{NC}$ 群. 因而 $\overline{G}=\Omega_1(\overline{G})$. 故 G/G' 初等交换. 因而 $G'=\Phi(G)$.

若 $Z(G)\nleqslant\Phi(G)$, 由于 G 是非交换的, 故存在 $1\neq N\leqslant G$ 使得 $G=Z(G)N$ 且 $Z(G)\bigcap N=1$. 明显地, $N\trianglelefteq G$. 故 $Z(G)\bigcap N\neq 1$, 矛盾. 于是 $Z(G)\leqslant\Phi(G)$. □

定理 14.16.2 的直接推论是如下.

推论 14.16.3 设 G 是有限 p 群.

(1) 若 $\Omega_1(G)\leqslant M\lessdot G$, 则 M 在 G 中无补.

(2) 若 G 是正则的 $\mathcal{NC}$ 群, 则 $\exp(G)=p$. 特别地, 若 G 是交换的 $\mathcal{NC}$ 群, 则 G 是初等交换的.

定理 14.16.4 设 G 是 p 群, $|G'|=p$. 则 G 是 $\mathcal{NC}$ 群当且仅当 $G\cong \mathrm{M}_p(1,1,1)$.

证明 $\Longleftarrow$: 显然.

$\Longrightarrow$: 由定理 14.16.2 可得, $Z(G)\leqslant G'$. 因为 $|G'|=p$ 且 $Z(G)>1$, 故 $G'=Z(G)$. 由定理 14.16.2 得 $G=\Omega_1(G)$. 因而存在 $a\in G$ 使得 $o(a)=p$ 且 $a\notin\Phi(G)$. 令 $H=\langle a\rangle G'$. 明显地, $|H|=p^2$. 又由定理 14.16.2 知 $G'=\Phi(G)$. 故 H 是不含在 $\Phi(G)$ 中的 G 的正规子群. 由假设, H 在 G 中有补 K. 因而 $|G:K|=|H|=p^2$. 因为 $K'\leqslant G'\bigcap K\leqslant H\bigcap K$ 且 $H\bigcap K=1$, 故 $K'=1$. 因而 K 交换. 于是 $KG'=KZ(G)$ 是 G 的交换极大子群. 由定理 1.7.6 可得 $|G|=p|Z(G)||G'|=p^3$. 于是 G 是内交换的. 又由定理 14.16.2 可知 $G=\Omega_1(G)$. 检查定理 1.7.10 中的群易得 $G\cong \mathrm{M}_p(1,1,1)$. □

引理 1.7.7 和定理 14.16.4 直接结果是如下推论.

推论 14.16.5 设 G 是 $\mathcal{A}_1$ 群. 则 G 是 $\mathcal{NC}$ 群当且仅当 $G\cong \mathrm{M}_p(1,1,1)$.

推论 14.16.6 设 G 是非交换的 $\mathcal{NC}$-p 群. 则 $d(G)=2$.

证明 若 $|G'|=p$, 由定理 14.12.2 可知, $G\cong \mathrm{M}_p(1,1,1)$. 于是 $d(G)=2$. 若 $|G'|\geqslant p^2$. 取 $N\lessdot G'$ 且 $N\trianglelefteq G$. 则 $|\overline{G}'|=|G'/N|=p$. 因为 $\mathcal{NC}$ 群的商群是 $\mathcal{NC}$ 群, 故 $\overline{G}=G/N$ 是 $\mathcal{NC}$ 群. 由定理 14.16.4 可得 $d(\overline{G})=2$. 因而 $d(G)=2$. □

引理 14.16.7 设 G 是 p 群, $d(G)=2$. 若 H 是 G 的不含在 $\Phi(G)$ 中的正规子群, 则 $G'\leqslant H$.

证明 因为 $H\nleqslant\Phi(G)$ 且 $d(G)=2$, 故存在 $a\in H\backslash\Phi(G)$ 和 $b\in G$ 使得 $G=\langle a,b\rangle$. 由 $H\trianglelefteq G$ 可得 $[a,b]=a^{-1}a^b\in H$. 于是 $G'=\langle [a,b]^g\mid g\in G\rangle\leqslant H$. □

定理 14.16.8 设 G 是有限 p 群. 则 G 是非交换的 $\mathcal{NC}$ 群当且仅当 $d(G)=2$, $G'=\Phi(G)$ 且 $G=\Omega_1(G)$.

证明 $\Longrightarrow$: 由定理 14.16.2 和推论 14.16.6 即得.

$\Longleftarrow$: 设 H 是 G 的不含在 $\Phi(G)$ 中的正规子群. 因为 $d(G)=2$, 由引理 14.16.7 可知 $G'\leqslant H$. 进一步地, 由 $G'=\Phi(G)$ 可知 H 是 G 的极大子群. 因为 $G=\Omega_1(G)$, 故存在 $a\in G$ 且 $o(a)=p$ 使得 $a\notin H$. 于是 $G=H\langle a\rangle$ 且 $H\bigcap\langle a\rangle=1$. 因而 H 在 G 中可补, 故 G 是 $\mathcal{NC}$ 群. □

定理 14.16.9　设 G 是非交换 2 群, 其阶为 2^n. 则 G 是 $\mathcal{NC}$ 群当且仅当 $G \cong \mathrm{D}_{2^n}$.

证明　$\Longleftarrow$: 设 $G \cong \mathrm{D}_{2^n}$. 为方便设

$$G = \langle a, b \mid a^{2^{n-1}} = 1, b^2 = 1, a^b = a^{-1} \rangle, \quad n \geqslant 3.$$

因为 $G = \langle ab, b \rangle$ 且 $o(ab) = o(b) = 2$, 故 $G = \Omega_1(G)$. 明显地, $d(G) = 2$ 且 $G' = \Phi(G)$. 由定理 14.16.8 可得 G 是 $\mathcal{NC}$ 群.

$\Longrightarrow$: 由推论 14.16.6 可得 $d(G) = 2$. 再由定理 14.16.8 得 $|G : G'| = 2^2$. 由定理 1.11.9 可知 G 是极大类的, 且 G 同构于下列群之一: D_{2^n}, 即二面体群; Q_{2^n}, 即广义四元数群以及 SD_{2^n}, 即半二面体群. 注意到对于 Q_{2^n} 有 $|\Omega_1(G)| = 2$, 而对于 SD_{2^n} 有 $|G : \Omega_1(G)| = 2$. 由定理 14.16.8 可知, G 不能同构于 Q_{2^n} 或 SD_{2^n}. 因而 $G \cong \mathrm{D}_{2^n}$. □

定理 14.16.9 告诉我们 $\mathcal{NC}$-2 群是极大类的. 自然地要问: 奇阶 $\mathcal{NC}$ 群是极大类 p 群吗? 例 14.16.1 告诉我们, 答案是否定的. 下面我们讨论奇阶 $\mathcal{NC}$ 群.

定理 14.16.10　设 G 是有限 p 群, $c(G) = 2$. 则 G 是 $\mathcal{NC}$ 群当且仅当 $G \cong \mathrm{M}_p(1,1,1)$.

证明　若 G 是 $\mathcal{NC}$ 群, 由定理 14.16.8 可知, $d(G) = 2, G = \Omega_1(G)$. 设 $G = \langle a, b \rangle$, 其中 $o(a) = o(b) = p$. 因为 $c(G) = 2$, 故 $G' \leqslant Z(G)$. 于是 $G' = \langle [a, b] \rangle$. 于是

$$[a, b]^p = [a^p, b] = 1.$$

故 $|G'| = p$. 由定理 14.16.4 可知, $G \cong \mathrm{M}_p(1,1,1)$. 反之, 结论明显地成立. □

定理 14.16.4 和定理 14.16.10 的一个直接结果如下.

推论 14.16.11　设 G 是 $\mathcal{NC}$ 群. 则下列陈述等价.

(1) G 是 $\mathcal{A}_1$ 群;

(2) $|G'| = p$;

(3) $c(G) = 2$;

(4) $G \cong \mathrm{M}_p(1,1,1)$.

下面分类 $\mathcal{NC}$-$\mathcal{A}_t$ 群, 其中 $t = 2$ 和 3. $\mathcal{A}_2$ 群和 $\mathcal{A}_3$ 群已被张勤海等分别在文献 [273],[280] 分类. 然而, 有一个长的群表, 文献 [229] 给了一个不依赖于查表的证明. 首先对 $\mathcal{NC}$-$\mathcal{A}_t$ 群的阶有以下结果.

定理 14.16.12　设 G 是 $\mathcal{A}_t$ 群, $t \geqslant 1$. 若 G 是 $\mathcal{NC}$ 群, 则 $|G| = p^{t+2}$.

证明　设 $|G| = p^n$. 只需证 $t = n - 2$ 即可, 即只需证 G 有 p^3 阶非交换子群.

令 $c = c(G)$. 若 $c = 2$, 则结论由推论 14.16.11 得出. 下设 $c \geqslant 3$. 因为 G 是 $\mathcal{NC}$ 群, 由定理 14.16.8 可知, $d(G) = 2$ 且 $G = \Omega_1(G)$. 不妨设 $G = \langle a, b \rangle$, 其中 $o(a) = o(b) = p$. 按以下三步证明结论.

(1) $\exp(G_c)=p$.

因为 $G_{c+1}=1$, 故 $G_c\leqslant Z(G)$. 由 $G_c=[G_{c-1},G]$ 可得

$$G_c=\langle [x,a],[x,b]\mid x\in G_{c-1}\rangle.$$

令 $x\in G_c$. 由 [89] 中的III, 引理 1.3 可知,

$$[x,a]^p=[x,a^p]=1,\quad [x,b]^p=[x,b^p]=1.$$

于是 $\exp(G_c)=p$.

(2) G_{c-1} 可由 p 阶元生成, 即 $G_{c-1}=\Omega_1(G_{c-1})$.

令 $x\in G_{c-2}$ 且 $H=\langle x,a\rangle$. 若 $c=3$, 则 G' 交换. 于是 H' 交换. 设 $c\geqslant 4$. 则

$$H'=\langle [x,a]^h\mid h\in H\rangle\leqslant G_{c-1}.$$

因为

$$[G_{c-1},G_{c-1}]\leqslant G_{2c-4}\leqslant G_c=1,$$

故 G_{c-1} 交换. 由此可得 H' 交换. 于是 H 亚交换. 由命题 1.1.9 和 (1) 可得

$$1=[x,a^p]=[x,a]^p[x,a,a]^{\binom{p}{2}}=[x,a]^p.$$

同样的论证可得 $[x,b]^p=1$. 因为

$$G_{c-1}=\langle [x,a]^g,[x,b]^g\mid x\in G_{c-2},\ g\in G\rangle,$$

故 $G_{c-1}=\Omega_1(G_{c-1})$.

(3) G 有 p^3 阶的内交换子群.

因为

$$G_c=\langle [x,a]^g,[x,b]^g\mid x\in G_{c-1},g\in G\rangle\neq 1,$$

由 (2) 可知, 存在 $x\in G_{c-1}$ 且 $o(x)=p$ 使得 $[x,a]\neq 1$ 或 $[x,b]\neq 1$. 不妨设 $[x,a]\neq 1$. 令 $H=\langle x,a\rangle$. 因为 $c(G)=c$, 故 $[x,a]\in Z(G)$. 从而 $H'=\langle [x,a]\rangle$. 由 (1) 得 $o([x,a])=p$. 再由定理 1.7.7(2) 得, H 是 G 的 p^3 阶的内交换子群. □

定理 14.16.13 设 G 是奇阶 $\mathcal{A}_2$ 群. 则 G 是 $\mathcal{NC}$ 群当且仅当 G 同构于下列群之一.

(1) $G=\langle a_1,b\mid a_1^p=a_2^p=a_3^p=b^p=1,[a_1,b]=a_2,[a_2,b]=a_3,[a_3,b]=[a_1,a_3]=[a_1,a_2]=1\rangle$;

(2) $G=\langle a_1,b\mid a_1^3=a_2^3=b^9=1,[a_1,b]=a_2,[a_2,b]=b^3,[a_1,a_2]=1\rangle$;

(3) $G=\langle a_1,b\mid a_1^9=a_2^3=b^3=1,[a_1,b]=a_2,[a_2,b]=a_1^{-3},[a_1,a_2]=1\rangle$.

证明　$\Longleftarrow$: 很清楚, 定理中的群均满足 $d(G)=2$ 且 $G'=\Phi(G)$. 对于群 (1), $G=\Omega_1(G)$. 注意到对于群 (2), $(a_1b^2)^3=1$; 对于群 (3), $(a_1b)^3=1$. 故 $G=\Omega_1(G)$. 由定理 14.16.8 可知, 定理中列出的群均是 $\mathcal{NC}$ 群.

$\Longrightarrow$: 因为 G 是 $\mathcal{A}_2$ 群又是 $\mathcal{NC}$ 群, 由定理 14.16.12 可知, $|G|=p^4$. 检查 p^4 阶群的分类即得定理中的群 (1)—(3). □

推论 14.16.14　*设 G 是 $\mathcal{NC}$-p 群. 则 $|G'|=p^2$ 当且仅当 G 是定理 14.16.13中列出的群之一.*

证明　明显地, 定理 14.16.13 中的群的导群均具有 p^2 阶. 反之, 若 $|G'|=p^2$, 由定理 1.7.7 可知, G 不是内交换的. 因为 G 是 $\mathcal{NC}$ 群, 由定理 14.16.8 可知, $|G|=p^4$. 于是 G 是 $\mathcal{A}_2$ 群. 此时结论由定理 14.16.13 推出. □

定理 14.16.15　*设 G 是奇阶 $\mathcal{A}_3$ 群. 则 G 是 $\mathcal{NC}$ 群当且仅当 G 同构于下列群之一.*

(1) $G=\langle a_1,b \mid a_1^p=a_2^p=a_3^p=a_4^p=b^p=1,[a_1,b]=a_2,[a_2,b]=a_3,[a_3,b]=a_4,[a_4,b]=1,[a_i,a_j]=1\rangle, p\geqslant 5, 1\leqslant i\leqslant 4, 1\leqslant j\leqslant 3$;

(2) $G=\langle a_1,b \mid a_1^p=a_2^p=a_3^p=a_4^p=b^p=1,[a_1,b]=a_2,[a_2,b]=a_3,[a_2,a_1]=a_4,[a_3,b]=a_4,[a_3,a_1]=[a_4,a_1]=[a_4,b]=1\rangle, p\geqslant 5$;

(3) $G=\langle a_1,b \mid a_1^p=b^p=a_2^p=a_3^p=a_4^p=1,[a_1,b]=a_2,[a_2,a_1]=a_3,[a_2,b]=a_4,[a_3,a_1]=[a_3,b]=[a_4,a_1]=[a_4,b]=1\rangle, p\geqslant 3$;

(4) $G=\langle a_1,b \mid a_1^9=a_2^9=1,b^3=a_2^3,[a_1,b]=a_2,[a_2,b]=a_2^{-3}a_1^{-3},[a_2,a_1]=a_2^3\rangle$;

(5) $G=\langle a_1,b \mid a_1^9=a_2^9=b^3=1,[a_1,b]=a_2,[a_2,b]=a_1^{-3}a_2^{-3},[a_1,a_2]=1\rangle$.

证明　$\Longleftarrow$: 很清楚, 定理中的群均满足 $d(G)=2$ 和 $G'=\Phi(G)$. 对于群 (1–3), $G=\Omega_1(G)$. 另一方面, 对于群 (4–5), 由命题 1.1.10 计算可得, $(a_1b^{-1})^3=1$. 于是 $G=\Omega_1(G)$. 由定理 14.16.8 可知, 定理中列出的群均是 $\mathcal{NC}$ 群.

$\Longrightarrow$: 因为 G 是 $\mathcal{A}_3$ 群又是 $\mathcal{NC}$ 群, 由定理 14.16.12 可知, $|G|=p^5$. 对于 $p\geqslant 5$, 检查文献 [270] 给出的分类, 对于 $p=3$, 使用 Magma 检查小群库中的群即得定理中的群 (1)—(5). □

注 14.16.16　*对于 $t\leqslant 3$, 由 $\mathcal{A}_t$ 群的分类可知, 有 3 类 $\mathcal{A}_1$ 群、22 类 $\mathcal{A}_2$ 群、222 类 $\mathcal{A}_3$ 群. 然而, 推论 14.16.5、定理 14.16.13 和定理14.16.15 告诉我们, $\mathcal{A}_t(t\leqslant 3)$群中仅有几个群是 $\mathcal{NC}$ 群. 这意味着 p 群 G 的不含在 $\Phi(G)$ 里的非平凡真正规子群有补这个假设对 p 群结构有很强的限制.*

参 考 文 献

[1] Abuhamda A H. Inductive isomorphisms of certain classes of groups (Russian). Math. Issled., 1975, 10, 1(35): 3–19, 293. MR 0476853(57 #16404).

[2] An L J, Qu H P, Xu M Y, Yang C S. Quasi-NC groups. Comm. Algebra, 2008, 36(11): 4011–4019.

[3] 安立坚. 有限亚 Hamilton p 群的完全分类. 北京大学博士学位论文, 2009.

[4] 安立坚, 魏军军. 满足 $|\mathrm{I}_3(G)| = 4$ 的有限 2 群的完全分类. 数学的实践与认识, 2010, 40(22): 237–242.

[5] 安立坚, 成小院. 交换子群较小的一类有限 p 群. 数学研究, 2011, 44(1): 107–110.

[6] An L J, Ding J F, Zhang Q H. Finite self dual groups. J. Algebra, 2011, 341: 35–44.

[7] An L J, Peng J. Finite p-groups in which any two noncommutative elements generate an inner abelian group of order p^4. Algebra Colloq., 2013, 20(2): 215–226.

[8] An L J, Li L L, Qu H P, Zhang Q H. Finite p-groups with a minimal non-abelian subgroup of index p (Ⅱ). Sci. China Math., 2014, 57(4): 737–753.

[9] An L J, Hu R F, Zhang Q H. Finite p-groups with a minimal nonabelian subgroup of index p (Ⅳ). J. Algebra Appl., 2015, 14(2): 1550020(54 pages).

[10] An L J, Zhang Q H. Finite metahamiltonian p-groups. J. Algebra, 2015, 442: 23–35.

[11] An L J, Yang L. The central extension of an elementary abelian p-group by a minimal non-abelian p-group. J. Math. Res. Appl., 2016, 36(4): 457–466.

[12] Arad Z, Ward M B. New criteria for the solvability of finite groups. J. Algebra, 77(1): 1982: 234–246.

[13] Bacon M R. Kappe L C. The nonabelian tensor square of a 2-generator p-group of class 2. Arch. Math.(Basel), 1993, 61(6): 508–516.

[14] Baer R. Situation der untergruppen und struktur der gruppe. Sitz. Ber. Heidelberg Akad., 1933, 2: 12–17.

[15] Baer R. Der Kern, eine charakteristiche Untergruppe. Compositio Math., 1935, 1: 254–283. MR1556893.

[16] Baer R. Groups with abelian norm quotient group. Amer. J. Math., 1939, 61(3): 700–708.

[17] Bagnera G. La composizione dei Gruppi finiti il cui grado é la quinta potenza di un numero primo. Ann. Math. Pura Appl., 1898, 1(1): 137–228.

[18] Bai H, Ma Y J, Zhang J P. The coexponent of a finite p-group, Comm. Algebra, 2003, 31(7): 3497–3504.

[19] Ballester-Bolinches A, Guo X Y. On complemented subgroups of finite groups. Arch. Math., 1999, 72(3): 161–166.

[20] Bechtell H. On the structure of solvable nC-groups. Rend. Sem. Mat. Univ. Padova, 1972, 47: 13–22.

[21] Bechtell H, Deaconescu M, Silberberg G. Finite groups with large automizers for their abelian subgroups. Canad. Math. Bull., 1997, 40(3): 266–270.

[22] Bender H A. A determination of the groups of order p^5. Ann. Math., 1927/1928, 29(2): 61–72.

[23] Berkovich Y. On subgroups of finite p-groups. J. Algebra, 2000, 224(2): 198–240.

[24] Berkovich Y. Short proofs of some basic characterization theorems of finite p-group theory. Glas. Mat. Ser. III, 2006, 41(61): 239–258.

[25] Berkovich Y, Janko Z. Structure of finite p-groups with given subgroups. Contemp. Math., 2006, 402: 13–93.

[26] Berkovich Y. Groups of Prime Power Order Vol.1. Berlin: Walter de Gruyter, 2008.

[27] Berkovich Y, Janko Z. Groups of Prime Power Order Vol.2. Berlin: Walter de Gruyter, 2008.

[28] Berkovich Y, Janko Z. Groups of Prime Power Order Vol.3. Berlin: Walter de Gruyter, 2011.

[29] Besche H U, Eick B, O'Brien E A. A millennium project: constructing small groups. Internat. J. Algebra Comput., 2002, 12(5): 623–644.

[30] Blackburn N. On prime-power groups in which the derived group has two generators. Proc. Cambr. Phil. Soc., 1957, 53: 19–27.

[31] Blackburn N. Generalizations of certain elementary theorems on p-groups. Proc. London Math. Soc., 1961, 11(3): 1–22.

[32] Blacburn N. Finite groups in which the nonnormal subgroups have nontrival intersection. J. Algebra, 1966, 3: 30–37.

[33] Blackburn N, Deaconescu M, Mann A. Finite equilibrated groups. Math. Proc. Cambridge. Philos. Soc., 1996, 120(4): 579–588.

[34] Blackburn N, Héthelyi L. Some further properties of soft subgroups. Arch. Math.(Basel), 1997, 69(5): 365–371.

[35] Blackburn S R. Enumeration within isoclinism classes of groups of prime power order. J. London Math. Soc., 1994, 50(2): 293–304.

[36] Blackburn S R. Groups of prime power order with derived subgroup of prime order. J. Algebra, 1999, 219(2): 625–657.

[37] Bosma W, Cannon J, Playoust C. The Magma algebra system I: The user language. J. Symbolic Comput., 1997, 24(3-4): 235–265.

[38] Božikov Z, Janko Z. Finite 2-groups with exactly one maximal subgroup which is neither abelian nor minimal nonabelian. Glas. Mat. Ser. III, 2010, 45(65): 63–83.

[39] Bradway R H, Gross F, Scott W R. The nilpotence class of core-free quasinormal subgroups. Rocky Mountain J. Math., 1971, 1(2): 375–382.

[40] Brandl R. Groups with few non-normal subgroups. Comm. Algebra, 1995, 23(6): 2091–2098.

[41] Brandl R, Deaconescu M. Finite groups with small automizers of their nonabelian subgroups. Glasg. Math. J., 1999, 41(1): 59–64.

[42] Brandl R. Conjugacy classes of non-normal subgroups of finite p-groups. Israel J. Math., 2013, 195(1): 473–479.

[43] Bryce R A, Cossey J, Ormerod E A. A note on p-groups with power automorphisms. Glasgow Math. J., 1992, 34(3): 327–332.

[44] Cao J J, Guo X Y. Finite soluble groups in which the normalizer of every nonnormal cyclic subgroup is maximal. J. Group Theory, 2014, 17(4): 671–687.

[45] Cappitt D. Generalized Dedekind groups. J. Algebra, 1971, 17(3): 310–316.

[46] Černikov S N. Groups with systems of complemented subgroups. Doklady Akad. Nauk. SSSR (N. S.), 1953, 92: 891–894. MR0059276(15 #504a).

[47] 陈贵云, 陈顺民. 非正规子群共轭类类数为 2 的有限群的一个注记. 吉林大学学报, 2008, 46(6): 1097–1100.

[48] Cheng Y. On finite p-groups with cyclic commutator subgroup. Arch. Math.(Basel), 1982, 39(4): 295–298.

[49] Cheng Y. On double centralizer subgropups of some finite p-groups. Proc. Amer. Math. Soc., 1982, 86(2): 205–208.

[50] 陈重穆. 关于正则 p 群幂零类的一个注记. 西南师范大学学报 (自然科学版), 1988, 2: 1–4.

[51] Christensen C. Complementation in groups. Math. Z., 1964, 84: 52–69.

[52] Christensen C. Groups with Complemented Normal Subgroups. J. London Math. Soc., 42: 1967, 208–216.

[53] Cooper C D H. Power automorphisms of a group. Math. Z., 1968, 107: 335–356.

[54] Cossey J, Stonehewer S E. Cyclic permutable subgroups of finite groups. J. Aust. Math. Soc., 2001, 71(2): 169–176.

[55] Cossey J, Stonehewer S E. The embedding of a cyclic permutable subgroup in a finite group. Special issue in honor of Reinhold Baer (1902–1979), Illinois J. Math., 2003, 47(1-2): 89–111.

[56] Deaconescu M, Mazurov V D. Finite groups with large automizers for their nonabelian subgroups. Arch. Math.(Basel), 1997, 69(6): 441–444.

[57] Dedekind R. Über Gruppen, deren sämmtliche Theiler Normaltheiler sind. Math. Ann., 1897, 48(4): 548–561. MR1510943.

[58] Deskins W E. On quasinormal subgroups of finite groups. Math. Z., 1963, 82: 125–132.

[59] De Séguier J-A. Théorie des groupes finis. Éléments de la théorie des groupes abstraits, Gauthier-Villars, Paris, 1904.

[60] Dixon J D, du Sautoy M P F, Mann A, Segal D. Analytic pro-p-groups. London Math. Soc. Lecture Note Ser. 157, Cambridge: Cambridge University Press, 1991.

[61] Fang X G, An L J. A classification of finite meta-Hamilton p-groups. Submitted to Sci. China Math.

[62] Fernández-Alcober G A, Legarreta L. The finite p-groups with p conjugacy classes of non-normal subgroups. Israel J. Math., 2010, 180: 189–192.

[63] Finogenov A A. Finite p-groups with a cyclic commutator group (Russian). Algebra i Logika, 1995, 34(2): 233–240, 243; translation in Algebra and Logic, 1995, 34(2) 125–129. MR1362616 (96k:20036).

[64] Finogenov A A. On finite p-groups with a cyclic commutator group and cyclic center(Russian). Mat. Zametki, 1998, 63(6): 911–922; translation in Math. Notes, 1998, 63(5): 802–812. MR1679224 (2000a:20044).

[65] Foguel T. Conjugate-permutable subgroups. J. Algebra, 1997, 191(1): 235–239.

[66] Foguel T. Groups with all cyclic subgroups conjugate-permutable groups. J. Group Theory, 1999, 2(1): 47–51.

[67] Gheorghe P. On the structure of quasi-Hamiltonian groups. Acad. Repub. Pop. Române. Bul. Sti. A., 1949, 1: 973–979. MR0045114(13 #529c)

[68] Golovanov M I. Finite p-groups with the condition $|\,\mathrm{I}_m(P)| = p^{m-1}$. (Russian) Some questions on the theory of groups and rings (Russian). Inst. Fiz. im. Kirenskogo Sibirsk. Otdel. Akad. Nauk SSR, Krasnoyarsk, 1973: 58–82, 175.

[69] Gorenstein D. Finite Groups. New York: Chelsea Publishing Co, 1980.

[70] Gross F. p-subgroups of core-free quasinormal subgroups. Rocky Mountain J. Math., 1971, 1(3): 541–550.

[71] Gross F, Berger T R. A universal example of a core-free permutable subgroup. Rocky Mountain J. Math., 1982, 12(2): 345–365.

[72] Guo X Y, Shum K P. Complementarity of subgroups and the structure of finite groups. Algebra Colloq., 2006, 13(1): 9–16.

[73] Guo X Y, Wang J X. On generalized Dedekind groups. Acta Math. Hungar., 2009, 122(1-2): 37–44.

[74] Guo X Y, Zhao L B. On J-groups of prime power order. J. Algebra Appl., 2012, 11(6): 1250106(11 pages).

[75] Guo X Y, Zhang X H. On the norm and Wielandt series in finite groups. Algebra Colloq., 2012, 19(3): 411–426.

[76] Hall M Jr, Senior J K. The groups of order $2^n (n \leqslant 6)$. New York: The Macmillan Co., 1964.

[77] Hall P. A contribution to the theory of groups of prime-power order. Proc. London Math. Soc., 1933, 36: 29–95.

[78] Hall P. A characteristic property of soluble groups. J. London Math. Soc., 1937, S1-12(2): 198–200.

[79] Hall P. Complemented groups. J. London Math. Soc., 1937, S1-12(2): 201–204.

[80] Hao C G, Jin Z X. Finite p-groups which contain a self-centralizing cyclic normal subgroup. Acta. Math. Sci. Ser. B, 2013, 33(1): 131–138.

[81] Hawidi H M, Sergeĭčuk V V. Two semiclassifying theorems for metabelian groups. Delta J. Sci., 1988, 12(1): 31–43. MR1025630 (90k:20038).

[82] Herzog M, Longobardi P, Maj M, Mann A. On generalized Dedekind groups and Tarski super Monsters. J. Algebra, 2000, 226(2): 690–713.

[83] Héthelyi L. Soft subgroups of p-groups. Ann. Univ. Sci. Budapest. Eötvös Sect. Math., 1984, 27: 81–85. MR0823095 (87c:20044).

[84] Héthelyi L. On subgroups of p-groups having soft subgroups. J. London Math. Soc., 1990, 41(3): 425–437.

[85] Héthelyi L. Some remarks on 2-groups having soft subgroups. Studia Sci. Math. Hungar., 1992, 27(3-4): 295–299. MR1218150 (94c:20036).

[86] Hobby C R. A characteristic subgroup of a p-group. Pacific J. Math., 1960, 10: 853–858.

[87] Huppert B. Über das Produkt von paarweise vertauschbaren zyklischen Gruppen. Math. Z., 1953, 58: 243–264. MR0055341 (14 #1059f).

[88] Huppert B. Zur Sylowstruktur auflösbarer Gruppen. Arch. Math.(Basel), 1961, 12: 161–169. MR0142641(26 #210).

[89] Huppert B. Endliche Gruppen I. Berlin: Springer-Verlag, 1967.

[90] Isaacs I M. Character Theory of Finite Groups. New York: Academic Press, 1976.

[91] Ishikawa K. Finite p-groups up to isoclinism, which have only two conjugacy lengths. J. Algebra, 1999, 220(1): 333–345.

[92] Itô N, Szép J. Über die Quasinormalteiler von endlichen Gruppen. Acta Sci. Math. (Szeged), 1962, 23: 168–170. MR0138676 (25 #2119).

[93] Iwasawa K. Über die endliche Gruppen und die Verbände ihrer Untergruppen. J. Fac. Sci. Imo. Univ. Tokyo, 1941, 4: 171–199. MR0005621(3 #193h).

[94] James R. The Groups of Order $p^6 (p \geqslant 3)$. University of Sydney Philosophic Doctor Thesis, 1968.

[95] James R. The groups of order p^6 (p an odd prime). Math. Comp., 1980, 34(150): 613–637.

[96] Janko Z. Finite p-groups with a uniqueness condition for non-normal subgroups. Glas. Mat. Ser. III, 2005, 40(60): 235–240.

[97] Janko Z. Minimal non-quaternion-free finite 2-groups. Israel J. Math., 2006, 154: 185–189.

[98] Janko Z. Some peculiar minimal situations by finite p-groups. Glas. Mat. Ser. IiI, 2008, 43(63): 111–120.

[99] Janko Z. Finite 2-groups with exactly one nonmetacyclic maximal subgroup. Israel J. Math., 2008, 166: 313–347.

[100] Janko Z. Finite p-groups G with $p > 2$ and $d(G) = 2$ having exactly one maximal subgroup which is neither abelian nor minimal nonabelian. Glas. Mat. Ser. III, 2010,

45(65): 441–452.

[101] Janko Z. Finite p-groups G with $p > 2$ and $d(G) > 2$ having exactly one maximal subgroup which is neither Abelian nor minimal nonAbelian. Glas. Mat. Ser. III, 2011, 46(66): 103–120.

[102] Janko Z. Finite p-groups all of whose proper subgroups have its derived subgroup of order at most p. Glas. Mat. Ser. III 2011, 46(66): 351–356.

[103] Janko Z. Finite nonabelian p-groups having exactly one maximal subgroup with a noncyclic center. Arch. Math.(Basel), 2011, 96(2): 101–103.

[104] Janko Z. Finite p-groups all of whose maximal subgroups, except one, have its derived subgroup of order $\leqslant p$. Glas. Mat. Ser. III, 2012, 47(67): 325–332.

[105] Janko Z. Finite nonabelian p-groups all of whose subgroup are q-self dual. J. Algebra Appl., 2014, 13(6): 1450008(7 pages).

[106] Janko Z. Finite p-groups all of whose maximal subgroups, except one, have cyclic derived subgroups. J. Algebra Appl., 2015, 14(1): 1450080(8 pages).

[107] Ji Y H, Du S F, Zhang L L. A classification of regular p-groups with invariants $(e, 2, 1)$. Southeast Asian Bull. Math., 2001, 25(2): 245–256.

[108] Kappe L C, Visscher M P, Sarmin N H. Two-generator two-groups of class two and their nonabelian tensor squares. Glasg. Math. J., 1999, 41(3): 417–430.

[109] Kappe L C, Kirtland J. Supplementation in groups. Glasg. Math. J., 2000, 42(1): 37–50.

[110] Kappe L C, Reboli D M. On the structure of generalized Hamiltonian groups. Arch. Math.(Basel), 2000, 75(5): 328–337.

[111] Kappe L C, Kirtland J. Finite groups with trivial Frattini subgroup. Arch. Math.(Basel), 2003, 80(3): 225–234.

[112] Khukhro E I. Mazurov V D. Unsolved problems in group theory. The Kourovka notebook, Novosibirsk, 2006, 16.

[113] King B W. Presentations of metacyclic groups. Bull. Aust. Math. Soc., 1973, 8: 101–131.

[114] Kirtland J. On two classes of finite inseparable p-groups. Acta Math. Sinica, Engl. Ser., 2015, 31(7): 1203–1214.

[115] Kurzweil H. Endliche Gruppen. Berlin-New York: Springer-verlag, 1977.

[116] Kurzweil H, Stellmacher B. The Theory of Finite Groups. New York: Universitext, Springer-verlag, 2004. An introduction; Translated from the 1998 German original.

[117] La Haye R, Rhemtulla A. Groups with a bounded number of conjugacy classes of non-normal subgroups. J. Algebra, 1999, 214(1): 41–63.

[118] Laffey T J. The minimum number of generators of a finite p-group. Bull. London Math. Soc., 1973, 5: 288–290.

[119] Lennox J C, Wiegold J. On a question of Deaconescu about automorphisms. Rend.

Sem. Math. Univ. Padova, 1993, 99: 83–86. MR1229044 (94f:20073).

[120] Leone A. Minimal non-KC finite p-groups(Italian). Matematiche (Catania), 1983, 38(1-2): 191–200. MR0924106 (89b:20050).

[121] 李立莉, 曲海鹏, 陈贵云. 内交换 p 群的中心扩张 (I). 数学学报, 2010, 53(4): 675–684.

[122] Li L L, Chen G Y. Minimal non self duan groups. Canad. Math. Bull., 2015，58(3): 538–547.

[123] Li L L, Qu H P. The number of conjugacy classes of nonnormal subgroups of finite p-groups. J. Algebra, 2016, 466: 44–62.

[124] 李璞金. 内 $\mathcal{P}_n$-p 群. 厦门大学博士学位论文, 2013.

[125] Li P J. A classification of finite p-groups whose proper subgroups are of class $\leqslant 2$ (I). J. Algebra Appl., 2013, 12(3): 1250170(22 pages).

[126] Li P J. A classification of finite p-groups whose proper subgroups are of class $\leqslant 2$ (II). J. Algebra Appl., 2013, 12(3): 1250171(29 pages).

[127] Li P J, Qu H P, Zeng J W. Finite p-groups whose proper subgroups are of class $\leqslant n$. J. Algebra Appl., 2017, 16(1): 1750014(8 pages).

[128] Li S R. The structure of NC-groups. J. Algebra, 2001, 241(2): 611–619.

[129] Li S R. Finite 2-groups with large centralizers of abelian subgroups. Math. Proc. Royal Irish Acad., 2004, 104A(2): 191–197.

[130] Li S R, Meng Z C. Groups with conjugate-permutable conditions. Math. Proc. Royal Irish Acad., 2007, 107A(2): 115–121.

[131] Li S R, Guo X Y. Finite p-groups whose abelian subgroups have a trivial intersection. Acta Math. Sinica Engl. Ser., 2007, 23(4): 731–734.

[132] Li T Z. A simple example of two p-groups with the same automorphism group. Arch. Math.(Basel), 2009, 92(4): 287–290.

[133] Li X H, Zhang J Q. Finite p-groups and centeralizers of noncentral elements. Comm. Algebra, 2013, 41(9): 3267–3276.

[134] Li X H, Zhang J Q. Finite p-groups with non-normal subgroups of index p in their normalizers. Comm. Algebra, 2011, 39(6): 2037–2043.

[135] Li Y M, Su N, Wang Y M. Complemented subgroups and the structure of finite groups. Monatsh Math., 2014, 173(3): 361–370.

[136] 吕恒, 陈贵云. 一类特殊的有限 p 群. 东北师大学报 (自然科学版), 2007, 39(2): 19–21.

[137] Lv H, Chen G Y. On Cernikov p-groups. Discrete Math., 2007, 308(21): 4992–4997.

[138] Lv H, Zhou W, Guo X Y. Finite 2-groups with index of every cyclic subgroup in its normal closure no greater than 4. J. Algebra, 2011, 342: 256–264.

[139] Lv H, Zhou W, Yu D. Some finite p-groups with bounded index of every cyclic subgroup in its normal closure. J. Algebra, 2011, 338: 169–179.

[140] Lv H, Guo X Y, Zhou W. On groups with a $CC(n)$-subgroup. Commu. Algebra, 2013, 41(3): 1182–1187.

[141] 吕恒, 周伟, 郭秀云. 关于有限 p 群的正规闭包的一些条件. 中国科学: 数学, 2013, 43(11): 1103–1112.

[142] Lv H, Zhou W, Xu H J. Finite p-groups with small subgroups generated by two conjugate elements. Arch. Math.(Basel), 2013, 100(4): 301–308.

[143] Lv H, Zhou W, Guo X Y. Finite groups with small normal closure of cyclic subgroups. Comm. Algebra, 2014, 42(11): 4984–4996.

[144] Macdonald I D. Generalizations of a classical theorem on nilpotent groups. Illinois J. Math., 1964, 8: 556–570.

[145] Mahdavi K. On groups with every subgroup 2-subnormal. Arch. Math.(Basel), 1986, 47(4): 289–292.

[146] Mahdavianary S K. A classification of 2-genterator p-group, $p \geqslant 3$, with many subgroups 2-subnormal. Arch. Math.(Basel), 1984, 43(2): 97–107.

[147] Mann A. Groups with dense normal subgroup. Israel J. Math., 1968, 6: 13–25.

[148] Mann A. Finite groups with maximal normalizers. Illinois J. Math., 1968, 12: 67–75.

[149] Mann A. Regular p-groups I. Israel J. Math., 1971, 10: 471–477.

[150] Mann A. Regular p-groups II. Israel J. Math., 1973, 14: 294–303.

[151] Mann A. The power structure of p-groups I. J. Algebra, 1976, 42(1): 121–135.

[152] Mann A. Regular p-groups III. J. Algebra, 1981, 70(1): 89–101.

[153] Mann A. Some questions about p-groups. J. Aust. Math. Soc., 1999, 67(3): 356–379.

[154] Mann A. The power structure of p-groups II. J. Algebra, 2007, 318(2): 953–956.

[155] Meixner T. Power automorphisms of finite p-group. Israel J. Math., 1981, 38(4): 345–360.

[156] Meng H Y, Guo X Y. The absolute center of finite groups. J. Group Theory, 2015, 18(6): 887–904.

[157] Miao L. On complemented subgroups of finite groups. Czechoslovak Math. J., 2006, 56(3): 1019–1028.

[158] Miech R J. On p-groups with a cyclic commutator subgroup. J. Aust. Math. Soc., 1975, 20(2): 178–198.

[159] Miech R J. The metabelian p-groups of maximal class. Trans. Amer. Math. Soc., 1978, 236: 93–119.

[160] Miller G A. An extension of Sylow's theorem. Proc. London Math. Soc., 1905, S2-2(1): 142–143.

[161] Miller G A. Determination of all the groups of order 2^m which contain an odd number of cyclic subgroups of composite order. Trans. Amer. Math. Soc., 1905, 6(1): 58–62.

[162] Miyamoto M. Solvability of some groups. Hokkaido Math. J., 1982, 11(1): 106–110. MR0649830 (83e:20025).

[163] Mousavi H. On finite groups with few non-normal subgroups. Comm. Algebra, 1999, 27(7): 3143–3151.

[164] Mousavi H. Finite nilpotent groups with three conjugacy classes of non-normal subgroups. Institute for Advanced Studies in Basic Science, Seminar on Algebra, 2004, 16: 147–150.

[165] Nagrebeckǐ V T. Invariant coverings of subgroups. Ural Gos. Univ. Mat. Zap., 1966, 5: 91–100. MR 34 # 2669

[166] Nagrebeckǐ V T. Finite non-nilpotent groups, any non-abelian subgroup of which is invariant. Ural Gos. Univ. Mat. Zap., 1967, 6: 80–88. MR 36 # 3871.

[167] Nagrebeckǐ V T. Finite groups in which any non-nilpotent subgroups is invariant, Ural Gos. Univ. Mat. Zap., 1968, 6: 45–49. MR0269730 (42 #4625).

[168] Nakamura K. Über einige Beispiele der strukturen Quasinormalteiler einer p-Gruppe. Nagoya Math. J., 1968, 1: 97–103. MR0222172 (36 #5224).

[169] Nakamura K. Beziehungen zwischen den Normalteiler und Quasinormalteiler. Osaka J. Math., 1970, 7: 321–322. MR0277616 (43 #3349).

[170] Nakamura K. Characteristische Untergruppen von Quasinormalteilern. Arch. Math.(Basel), 1979, 32(6): 513–515. MR0550314(82k:20055).

[171] Napolitani F. Finite p-groups in which the minimal subgroups are quasinormal. Rend. Circ. Mat. Palerm. (2), 1979, 28(1): 44–46. MR0564548 (81g:20036).

[172] Ore O. Structures and group theory I. Duke Math. J., 1937, 3(2): 149–174.

[173] Ormerod E A. The Wielandt subgroup of metacyclic p-groups. Bull. Aust. Math. Soc., 1990, 42(3): 499–510.

[174] Ormerod E A. On the Wielandt length of metabelian p-groups. Arch. Math.(Basel), 1991, 57(3): 212–215.

[175] Ormerod E A. Groups of Wielandt length two. Math. Proc. Cambridge. Philos. Soc., 1991, 110(2): 229–244.

[176] Ormerod E A. Some p-groups of Wielandt length three. Bull. Austral. Math. Soc., 1998, 58(1): 121–136.

[177] Ormerod E A. A note on the Wielandt subgroup of a metabelian p-group. Comm. Algebra, 1999, 27(2): 621–627.

[178] Ormerod E A. Finite p-group in which every cyclic subgroup is 2-subnormal. Glasg. Math. J., 2002, 44(3): 443–453.

[179] Ormerod E A, Parmeggiani G. Finite p-groups with normal normalisers. Bull. Aust. Math. Soc., 2004, 69(1): 141–150.

[180] Parmeggiani G. On finite p-groups of odd order with many subgroup 2-subnormal. Comm. Algebra, 1996, 24(8): 2707–2719.

[181] Passman D S. Nonnormal subgroups of p-groups. J. Algebra, 1970, 15: 352–370.

[182] Pazderski G. Induktive Isomorphie von Gruppen, deren Kommutatorgruppe Primzahlordnung besitzt. Arch. Math.(Basel), 1983, 41(5): 410–418. MR0731616 (86b:20024).

[183] Qian G H, Wang Y M. A note on character kernels in finite groups of prime power order. Arch. Math.(Basel), 2008, 90(3): 193–199.

[184] Qiao S H, Isaacs I M, Li Y M. Complemented subgroups and p-nilporence in finite groups. Arch. Math.(Basel), 2012, 98(5): 403–411.

[185] 曲海鹏. 具有指数为 2 的循环子群的亚循环群. 数学的实践与认识, 2009, 38(4): 215–217.

[186] 曲海鹏, 陈迎光. 9 中心化子群的结构. 数学研究, 2010, 43(1): 89–97.

[187] Qu H P. Finite p-groups all of whose maximal normal abelian subgroups are soft. Sci. China Math., 2010, 53(11): 3037–3040.

[188] 曲海鹏, 张巧红. 极小非 3 交换 3 群的分类. 数学进展, 2010, 39(5): 599–607.

[189] Qu H P. A characterization of finite generalized Dedekind groups. Acta Math. Hungar., 2014, 143(2): 269–273.

[190] Qu H P, Xu M Y, An L J. Finite p-groups with a minimal non-abelian subgroup of index p (III). Sci. China Math., 2015, 58(4): 763–780.

[191] Reboli D M. On the classification of generalized Hamiltonian groups. In Proceedings Groups St. Andrews 1997 in Bath II, Lecture Note Series, London Math. Soc., 1999, 261: 624–632.

[192] Rédei L. Das "schiefe produkt" in der Gruppentheorie mit Anwendung auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören. Comment. Math. Helv., 1947, 20: 225–264. MR0021933(9 #131a).

[193] Robinson D J S. A Course in the Theory of Groups. New York: Springer-Verlag, 1982.

[194] Roseblade J E. On groups in which every subgroup is subnormal. J. Algebra, 1965, 2: 402–412.

[195] Sanders P J, Wilde T S. The class and coexponent of a finite p-group. Technical Report, Mathematics Institute, University of Warwick, 1994.

[196] Sanders P J, Wilde T S. A bound for the nilpotency class of a finite p-groups in terms of its coexponent. arxiv: math. GR/9809153 v1 27 Sep., 1998: 1–7.

[197] Sanders P J. The coexponent of a regular p-group. Comm. Algebra, 2000, 28(3): 1309–1333.

[198] Schenkman E. On the norm of a group. Illinois J.Math., 1960, 4: 150–152.

[199] Schmidit O. Y. Groups having only one class of nonnormal subgroups(Russian). Mat. Sb, 1926, 33: 161–172.

[200] Schmidit O. Y. Groups with two classes of nonnormal subgroups(Russian). Proc.Seminar on Group Theory, 1938, 33: 7–26.

[201] Schreier O. Über die Erweiterung von Gruppen II. Abh. Math. Sem. Univ. Hamburg, 1926, 4(1): 321–346. MR3069457.

[202] Sergeĭčuk V V. The classification of metabelian p-groups. Matrix problems (Russian). 1977: 150–161. Akad. Nauk Ukrain. SSR Inst. Mat., Kiev, 1977. MR0491938 (58

#11109).

[203] Shalev A. On almost fixed point free automorphisms. J. Algebra, 1993, 157(1): 271–282.

[204] Silberberg G. Finite equilibrated 2-generated 2-groups. Acta Math. Hungar., 2006, 110(1-2): 23–35.

[205] 宋蕾薇, 曲海鹏. 所有子群皆循环或正规的有限 2 群. 数学的实践与认识, 2008, 38(10): 191–197.

[206] Song Q W, Qu H P, Guo X Y. Finite p-groups of class 3 all of whose proper sections have class at most 2. Algebra Colloq., 2010, 17(2): 191–201.

[207] 宋蕾薇, 崔双双. 某些 MI 群. 数学研究, 2011, 44(4): 387–392, 417.

[208] Song Q W, Xue F F. Finite p-groups which have a maximal subgroup is full-normal($p > 2$). Intern. J. Algebra, 2011, 5(29): 1421–1426.

[209] Song Q W. Finite two-generator p-groups with cyclic derived group. Comm. Algebra, 2013, 41(4): 1499–1513.

[210] Spencer A E. Self dual finite groups. Ist. Veneto Sci. Lett. Arti Atti Cl. Sci. Mat. Natur., 1971/72, 130: 385–391. MR0322052 (48 #416).

[211] Stonehewer S E. Permutable subgroups of some finite p-groups. Collection of articles dedicated to the memory of Hanna Neumann, I. J. Aust. Math. Soc., 1973, 16: 90–97.

[212] Stonehewer S E. Permutable subgroups of some finite permutation groups. Proc. London Math. Soc., 1974, 28(3): 222–236.

[213] Stonehewer S E, Zacher G. Abelian quasinormal subgroups of groups. Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl., 2004, 15(2): 69–79. MR2148535 (2007a:20022).

[214] Stonehewer S E. Old, recent and new results on quasinormal subgroups. Irish Math. Soc. Bull., 2005, 56: 125–133. MR2232103 (2007a:20018).

[215] Stonehewer S E, Zacher G. Cyclic quasinormal subgroups of arbitrary groups. Rend. Sem. Mat. Univ. Padova, 2006, 115: 165–187. MR2245594 (2007c:20069).

[216] The GAP Groups, Algorithms, and Programming. Version 4.4.7, http://www.gap-system.org, 2006.

[217] Thompson J G. An example of core-free quasinormal subgroup of p-groups. Math. Z., 1967, 96: 226–227.

[218] Višneveckiĭ A L. Groups of class 2 and exponent p with commutant of order p^2 (Russian). Dokl. Akad. Nauk Ukrain. SSR Ser. A, 1980, 9: 9–11, 103. MR0593560 (82d:20026).

[219] van der Waall R W. On finite p-groups whose commutator subgroups are cyclic. Nederl. Akad. Wetersch. Proc. Ser. A, 1973, 76: 342–345. MR0325765 (48 #4111).

[220] Walls G. Trivial intersection groups. Arch. der Math.(Basel), 1979, 32(1): 1–4.

[221] Wang J, Guo X Y. Finite p-groups and the centralizers of noncyclic abelian subgroups.

Bull Iran Math. Soc., 2017, 43(1): 171–192.

[222] Wang J, Guo X Y. On finite 2-equilibrated p-groups. J. Group Theory, 2016, 19(4): 569–588.

[223] Wang J X, Guo X Y. On the norm of finite groups. Algebra Colloq., 2007, 14(4): 605–612.

[224] Wang J X, Guo X Y. Finite groups with its power automorphism groups having small indices. Acta Math. Sinica, Engl. Ser., 2009, 7: 1097–1108.

[225] Wang J X, Guo X Y. Finite groups with a pre-fixed-point-free power automorphism. Comm. Algebra, 2013, 41(9): 3241–3251.

[226] Wang L F, Wang Y M. On CN-groups and CT-groups. Proc. Inter. Conf. on Algebra 2010: 649–656, World Sci. Publ., Hackensack, NJ, 2012.

[227] Wang L F, Zhang Q H. Finite 2-groups whose non-abelian subgroups have the same center. J. Group Theory, 2014, 17(4): 689–703.

[228] Wang L F, Qu H P. Finite groups in which the normal closures of non-normal subgroups have the same order. J. Algebra Appl., 2016, 15(7): 1650125(15 pages).

[229] Wang L F, Zhang Q H. Finite p-groups with a class of complemented normal subgroups. Acta Math. Sinica, Engl. Ser., 2017, 33(2): 278–286.

[230] 王丽芳. 内交换子群满足某些条件的亚循环 p 群. 数学进展, 待发表.

[231] Wang L F. Finite p-groups whose non-abelian subgroups have the same center. Submitted to J. Korea Math. Soc..

[232] Wielandt H. Über den Normalisator der subnormalen Untergruppen. Math. Z., 1958, 69: 463–465. MR0102550(21 #1341).

[233] 王汝楫. 有限 p 群的幂结构. 数学学报, 1986, 29(6): 847–852.

[234] 王汝楫. p^{p+1} 阶亚交换的非正则群的幂结构. 首都师范大学学报 (自然科学版), 1996, 17(3): 15–20.

[235] Wilkinson D. The groups of exponent p and order $\geqslant p^7$ (p any prime). J. Algebra, 1988, 118(1): 109–119.

[236] 徐明曜. 关于有限正则 p 群. 北京大学本科毕业论文, 1964.

[237] 徐明曜, 杨燕昌. 有限 p-群的半 p-交换性和正则性. 数学学报, 1976, 19(4): 281–285.

[238] 徐明曜. 关于有限 3 群的幂结构. 数学学报, 1984, 27(6): 721–729.

[239] 徐明曜. 关于正则 p 群的幂零类. 西南师范学院学报 (自然科学版), 1985, 2: 14–18.

[240] Xu M Y. The power structure of finite p-groups. Bull. Aust. Math. Soc., 1987, 36(1): 1–10.

[241] 徐明曜. 有限群导引 (上). 北京: 科学出版社, 1987; 2 版, 2007.

[242] Xu M Y. P. Hall's basis theorem for regular p-groups and its application to some classification problems. Comm. Algebra, 1991, 19(4): 1271–1280.

[243] Xu M Y. A note on the p-center of a finite p-group. Algebra Colloq., 1994, 1(3): 271–272.

[244] 徐明曜, 黄建华, 李慧陵, 李世荣. 有限群导引 (下). 北京: 科学出版社, 1999.

[245] Xu M Y, Zhang Q H. On conjugate-permutable subgroups of a finite group. Algebra Colloq., 2005, 12(4): 669–676.

[246] Xu M Y, An L J, Zhang Q H. Finite p-groups all of whose non-abelian proper subgroups are generated by two elements. J. Algebra, 2008, 319(9): 3603–3620.

[247] 徐明曜, 曲海鹏. 有限 p 群. 北京: 北京大学出版社, 2010.

[248] 徐尚进. GAP 入门导引. 北京: 科学出版社, 2014.

[249] Xue H B, Lv H, Chen G Y. On a special class of finite p-groups of maximal class. Ital. J. Pure Appl. Math., 2014, 33: 279–284.

[250] Yu D P, Lv H, Chen G Y, Li J B. Finite p-groups determined by an inequality of the order of any two-elements generated subgroups. Ital. J. Pure Appl. Math., 2013, 31: 255–262.

[251] Yu D P, Chen G Y, Xue H B, Lv H. Finite p-groups in which normal closures for every nonnormal subgroups are minimal nonabelian. Ital. J. Pure Appl. Math., 2015, 34: 431–436.

[252] Zassenhaus H J. A group-theoretic proof of a theorem of Maclagan-Wedderburn. Proc. Glasgow Math. Assoc., 1952, 1: 53–63. MR0052407 (14,614f).

[253] Zappa G. Finite groups in which all nonnormal subgroups have the same order (Italian). Atti Accad. Lincei(9) Math. Appl., 2002, 13(1): 5–16. MR1949144(2003k:20024).

[254] Zappa G. Finite groups in which all nonnormal subgroups have the same order II (Italian). Atti Accad. Lincei(9) Math. Appl., 2003, 14(1): 13–21. MR2057271(2005b:20039).

[255] 张博儒, 郭秀云. 中心自同构集合是内自同构的有限 p 群. 上海大学学报 (自然科学版), 未发表.

[256] 张军强, 黎先华. 真子群的导群都较小的有限 p 群. 中国科学 (A 辑), 数学, 2009, 39(12): 1403–1408. English translation: Zhang J Q, Li X H. Finite p-groups all of whose proper subgroups have small derived subgroups. Sci. China Math., 2010, 53(5): 1357–1362.

[257] Zhang J Q, Li X H. Finite p-groups all of whose proper subgroups have cyclic Frattini subgroups. J. Group Theory, 2012, 15(2): 245–259.

[258] 张军强, 任鹏飞. 一些特殊的 p 核 p 群. 数学实践与认识, 2012, 42(1): 242–246.

[259] Zhang J Q. Finite groups all of whose non-normal subgroups possess the same order. J. Algebra Appl., 2012, 11(3): 1250053(7 pages).

[260] Zhang J Q. Lu R J, Li W T. Finite p-groups and normal closures of nonnormal subgroups. J. Math. Res. Appl., 2015, 35(5): 521–528.

[261] Zhang J Q, Zhang Q H. Finite p-groups all of whose minimal nonnormal subgroups posses large normal closures. Comm. Algebra, 2016, 44(2): 628–638.

[262] Zhang J Q. Finite p-groups all of whose nonnormal subgroups posses special normalizers. Bull. Malaysian Math. Sci. Soc., 2017, 40(1): 279–293.

[263] Zhang L H, Zhang J Q. Finite p-groups all of whose nonnormal abelian subgroups are cyclic. J. Algebra Appl., 2013, 12(8): 1350052(9 pages).

[264] Zhang L H, Wang J, Qu H P. Finite p-groups whose non-central cyclic subgroups have cyclic quotient groups in their centralizers. Bull. Korean Math. Soc., 2015, 52(2): 367–376.

[265] Zhang L H, Xia Y M, Zhang Q H. Finite p-groups all of whose maximal subgroups are either metacyclic or have a derived subgroup of order $\leqslant p$. Chin. Ann. Math. Ser.B, 2015, 36(1): 11–30.

[266] Zhang L H. The intersection of nonabelian subgroups of finite p-groups. J. Algebra Appl., 2017, 16(1): 1750020(9 pages).

[267] Zhang L H. The intersection of maximal subgroups which are not minimal nonabelian of finite p-groups. Comm. Algebra, 2017, 48(5): 3221–3230.

[268] 张勤海, 王俊新. 子群为拟正规或自正规的有限群. 数学学报. 1995, 38(3): 381–385.

[269] Zhang Q H. s-semipermutability and abnormality in finite groups. Comm. Algebra, 1999, 27(9): 4514–4524.

[270] 张勤海, 宋蔷薇, 徐明曜. 某些正则 p 群的分类和应用. 中国科学 A 辑, 2006, 36(1): 5–30. English translation: Zhang Q H, Song Q W, Xu M Y. A classification of some regular p-groups and its applications. Sci. China Math., 2006, 49(3): 366–386.

[271] 张勤海, 孙翠娟, 曲海鹏, 徐明曜. 有限二元生成平衡 p 群, 中国科学 A 辑. 2007, 37（3）: 355–360. English translation: Zhang Q H, Sun C J, Qu H P, Xu M Y. Finite 2-generator equilibrated p-groups. Sci. China Math., 2007, 50(6): 814–820.

[272] Zhang Q H, Cao J J, Xu M Y. A Note on Finite superspecial p-groups. Adv. Math. (China), 2008, 37(4): 494-498.

[273] Zhang Q H, Sun X J, An L J, Xu M Y. Finite p-groups all of whose subgroups of index p^2 are Abelian. Algebra Colloq., 2008, 15(1): 167–180.

[274] 张勤海, 邓立军, 徐明曜. 任意两个非交换元均生成 p^3 阶子群的有限 p 群. 数学物理学报, 2009, 29A(3): 737–740.

[275] Zhang Q H, Guo X Q, Qu H P, Xu M Y. Finite groups which have many normal subgroups. J. Korean Math. Soc., 2009, 46(6): 1165–1178.

[276] Zhang Q H, Wei J J. The intersection of subgroup of finite p-groups. Arch. Math.(Bsel), 2011, 96(1): 9–17.

[277] Zhang Q H, Gao J. Normalizers of nonnormal subgroups of finite p-groups. J. Korean Math. Soc., 2012, 49(1): 201–221.

[278] Zhang Q H, Su M J. Finite 2-groups whose nonnormal subgroups have orders at most 2^3. Front. Math. China, 2012, 7(5): 971–1003.

[279] Zhang Q H, Li X X, Su M J. Finite p-groups whose nonnormal subgroups have orders at most p^3. Front. Math. China, 2014, 9(5): 1169–1194.

[280] Zhang Q H, Zhao L B, Li M M, Shen Y Q. Finite p-groups all of whose subgroups of

index p^3 are abelian. Commun. Math. Stat., 2015, 3(1): 69–162.

[281] Zhang X H, Guo X Y. Finite p-groups whose non-normal cyclic subgroups have small index in their normalizers. J. Group Theory, 2012, 15(5): 641–659.

[282] Zhang X H, Guo X Y. On the Wielandt subgroup in a p-groups of maximal class. Chin. Ann. Math. Ser.B, 2012, 33(1): 83–90.

[283] Zhao L B, Guo X Y. Finite p-groups with exactly one $\mathcal{A}_1$-subgroup of given structure of order p^3. Acta Math. Sinica, Engl. Ser., 2013, 29(11): 2099–2011.

[284] Zhao L B, Guo X Y. Finite p-groups in which the normal closures of the nonnormal cyclic subgroups have small index. J. Algebra Appl., 2014, 13(2): 1350087(7 pages).

[285] 赵立博, 郭秀云. 特定阶的子群都同构且交换的有限 p 群. 应用数学与计算数学学报, 2013, 27(4): 517–521.

索　　引

B

半 p 交换群, 222
不可分群, 342

D

单列嵌入子群, 118

G

共轭置换子群, 141
广义极大类 p 群, 275
广义 Dedekind 群, 131

H

换位子群, 236

J

基本 s 自对偶, 294
极小非 $\mathcal{P}_n$ 群, 189
极小非 p 交换 p 群, 181

K

可补子群, 342
可分群, 342
可裂, 342

M

幂自同构群, 315

N

内 $\mathcal{P}_n$ 群, 200
拟正规子群, 141
拟 p 交换群, 222
拟 NC 群, 235

P

平衡群, 252

Q

强可分群, 342

R

软子群, 275

Z

置换子群, 141
自对偶, 291
自共轭置换子群, 142
自同构导子, 234

其　　他

CCP 群, 143
ECP 群, 142
J 群, 101, 144
n-单列子群, 118
n-Engel 条件, 155
NC 群, 235
nC 群, 342
$\mathcal{NC}$ 群, 342
Norm, 300
p 导群, 181
p 换位子, 181
p 换位子群, 181
p 中心, 181
q 自对偶, 291
s 自对偶, 291
T 群, 83
TI 子群, 138
Wielandt 长, 300
Wielandt 列, 300
Wielandt 子群, 300

《现代数学基础丛书》已出版书目

(按出版时间排序)

1 数理逻辑基础(上册) 1981.1 胡世华 陆钟万 著
2 紧黎曼曲面引论 1981.3 伍鸿熙 吕以辇 陈志华 著
3 组合论(上册) 1981.10 柯 召 魏万迪 著
4 数理统计引论 1981.11 陈希孺 著
5 多元统计分析引论 1982.6 张尧庭 方开泰 著
6 概率论基础 1982.8 严士健 王隽骧 刘秀芳 著
7 数理逻辑基础(下册) 1982. 8 胡世华 陆钟万 著
8 有限群构造(上册) 1982.11 张远达 著
9 有限群构造(下册) 1982.12 张远达 著
10 环与代数 1983.3 刘绍学 著
11 测度论基础 1983.9 朱成熹 著
12 分析概率论 1984.4 胡迪鹤 著
13 巴拿赫空间引论 1984.8 定光桂 著
14 微分方程定性理论 1985.5 张芷芬 丁同仁 黄文灶 董镇喜 著
15 傅里叶积分算子理论及其应用 1985.9 仇庆久等 编
16 辛几何引论 1986.3 J.柯歇尔 邹异明 著
17 概率论基础和随机过程 1986.6 王寿仁 著
18 算子代数 1986.6 李炳仁 著
19 线性偏微分算子引论(上册) 1986.8 齐民友 著
20 实用微分几何引论 1986.11 苏步青等 著
21 微分动力系统原理 1987.2 张筑生 著
22 线性代数群表示导论(上册) 1987.2 曹锡华等 著
23 模型论基础 1987.8 王世强 著
24 递归论 1987.11 莫绍揆 著
25 有限群导引(上册) 1987.12 徐明曜 著
26 组合论(下册) 1987.12 柯 召 魏万迪 著
27 拟共形映射及其在黎曼曲面论中的应用 1988.1 李 忠 著
28 代数体函数与常微分方程 1988.2 何育赞 著
29 同调代数 1988.2 周伯壎 著

30　近代调和分析方法及其应用　1988.6　韩永生　著
31　带有时滞的动力系统的稳定性　1989.10　秦元勋等　编著
32　代数拓扑与示性类　1989.11　马德森著　吴英青　段海鲍译
33　非线性发展方程　1989.12　李大潜　陈韵梅　著
34　反应扩散方程引论　1990.2　叶其孝等　著
35　仿微分算子引论　1990.2　陈恕行等　编
36　公理集合论导引　1991.1　张锦文　著
37　解析数论基础　1991.2　潘承洞等　著
38　拓扑群引论　1991.3　黎景辉　冯绪宁　著
39　二阶椭圆型方程与椭圆型方程组　1991.4　陈亚浙　吴兰成　著
40　黎曼曲面　1991.4　吕以辇　张学莲　著
41　线性偏微分算子引论(下册)　1992.1　齐民友　许超江　编著
42　复变函数逼近论　1992.3　沈燮昌　著
43　Banach 代数　1992.11　李炳仁　著
44　随机点过程及其应用　1992.12　邓永录等　著
45　丢番图逼近引论　1993.4　朱尧辰等　著
46　线性微分方程的非线性扰动　1994.2　徐登洲　马如云　著
47　广义哈密顿系统理论及其应用　1994.12　李继彬　赵晓华　刘正荣　著
48　线性整数规划的数学基础　1995.2　马仲蕃　著
49　单复变函数论中的几个论题　1995.8　庄圻泰　著
50　复解析动力系统　1995.10　吕以辇　著
51　组合矩阵论　1996.3　柳柏濂　著
52　Banach 空间中的非线性逼近理论　1997.5　徐士英　李　冲　杨文善　著
53　有限典型群子空间轨道生成的格　1997.6　万哲先　霍元极　著
54　实分析导论　1998.2　丁传松等　著
55　对称性分岔理论基础　1998.3　唐　云　著
56　Gel'fond-Baker 方法在丢番图方程中的应用　1998.10　乐茂华　著
57　半群的 S-系理论　1999.2　刘仲奎　著
58　有限群导引(下册)　1999.5　徐明曜等　著
59　随机模型的密度演化方法　1999.6　史定华　著
60　非线性偏微分复方程　1999.6　闻国椿　著
61　复合算子理论　1999.8　徐宪民　著
62　离散鞅及其应用　1999.9　史及民　编著
63　调和分析及其在偏微分方程中的应用　1999.10　苗长兴　著

64 惯性流形与近似惯性流形 2000.1 戴正德 郭柏灵 著
65 数学规划导论 2000.6 徐增堃 著
66 拓扑空间中的反例 2000.6 汪 林 杨富春 编著
67 拓扑空间论 2000.7 高国士 著
68 非经典数理逻辑与近似推理 2000.9 王国俊 著
69 序半群引论 2001.1 谢祥云 著
70 动力系统的定性与分支理论 2001.2 罗定军 张 祥 董梅芳 编著
71 随机分析学基础(第二版) 2001.3 黄志远 著
72 非线性动力系统分析引论 2001.9 盛昭瀚 马军海 著
73 高斯过程的样本轨道性质 2001.11 林正炎 陆传荣 张立新 著
74 数组合地图论 2001.11 刘彦佩 著
75 光滑映射的奇点理论 2002.1 李养成 著
76 动力系统的周期解与分支理论 2002.4 韩茂安 著
77 神经动力学模型方法和应用 2002.4 阮炯 顾凡及 蔡志杰 编著
78 同调论——代数拓扑之一 2002.7 沈信耀 著
79 金兹堡-朗道方程 2002.8 郭柏灵等 著
80 排队论基础 2002.10 孙荣恒 李建平 著
81 算子代数上线性映射引论 2002.12 侯晋川 崔建莲 著
82 微分方法中的变分方法 2003.2 陆文端 著
83 周期小波及其应用 2003.3 彭思龙 李登峰 谌秋辉 著
84 集值分析 2003.8 李 雷 吴从炘 著
85 数理逻辑引论与归结原理 2003.8 王国俊 著
86 强偏差定理与分析方法 2003.8 刘 文 著
87 椭圆与抛物型方程引论 2003.9 伍卓群 尹景学 王春朋 著
88 有限典型群子空间轨道生成的格(第二版) 2003.10 万哲先 霍元极 著
89 调和分析及其在偏微分方程中的应用(第二版) 2004.3 苗长兴 著
90 稳定性和单纯性理论 2004.6 史念东 著
91 发展方程数值计算方法 2004.6 黄明游 编著
92 传染病动力学的数学建模与研究 2004.8 马知恩 周义仓 王稳地 靳 祯 著
93 模李超代数 2004.9 张永正 刘文德 著
94 巴拿赫空间中算子广义逆理论及其应用 2005.1 王玉文 著
95 巴拿赫空间结构和算子理想 2005.3 钟怀杰 著
96 脉冲微分系统引论 2005.3 傅希林 闫宝强 刘衍胜 著
97 代数学中的 Frobenius 结构 2005.7 汪明义 著

98 生存数据统计分析 2005.12 王启华 著
99 数理逻辑引论与归结原理(第二版) 2006.3 王国俊 著
100 数据包络分析 2006.3 魏权龄 著
101 代数群引论 2006.9 黎景辉 陈志杰 赵春来 著
102 矩阵结合方案 2006.9 王仰贤 霍元极 麻常利 著
103 椭圆曲线公钥密码导引 2006.10 祝跃飞 张亚娟 著
104 椭圆与超椭圆曲线公钥密码的理论与实现 2006.12 王学理 裴定一 著
105 散乱数据拟合的模型方法和理论 2007.1 吴宗敏 著
106 非线性演化方程的稳定性与分歧 2007.4 马 天 汪守宏 著
107 正规族理论及其应用 2007.4 顾永兴 庞学诚 方明亮 著
108 组合网络理论 2007.5 徐俊明 著
109 矩阵的半张量积:理论与应用 2007.5 程代展 齐洪胜 著
110 鞅与 Banach 空间几何学 2007.5 刘培德 著
111 非线性常微分方程边值问题 2007.6 葛渭高 著
112 戴维-斯特瓦尔松方程 2007.5 戴正德 蒋慕蓉 李栋龙 著
113 广义哈密顿系统理论及其应用 2007.7 李继彬 赵晓华 刘正荣 著
114 Adams 谱序列和球面稳定同伦群 2007.7 林金坤 著
115 矩阵理论及其应用 2007.8 陈公宁 著
116 集值随机过程引论 2007.8 张文修 李寿梅 汪振鹏 高 勇 著
117 偏微分方程的调和分析方法 2008.1 苗长兴 张 波 著
118 拓扑动力系统概论 2008.1 叶向东 黄 文 邵 松 著
119 线性微分方程的非线性扰动(第二版) 2008.3 徐登洲 马如云 著
120 数组合地图论(第二版) 2008.3 刘彦佩 著
121 半群的 S-系理论(第二版) 2008.3 刘仲奎 乔虎生 著
122 巴拿赫空间引论(第二版) 2008.4 定光桂 著
123 拓扑空间论(第二版) 2008.4 高国士 著
124 非经典数理逻辑与近似推理(第二版) 2008.5 王国俊 著
125 非参数蒙特卡罗检验及其应用 2008.8 朱力行 许王莉 著
126 Camassa-Holm 方程 2008.8 郭柏灵 田立新 杨灵娥 殷朝阳 著
127 环与代数(第二版) 2009.1 刘绍学 郭晋云 朱 彬 韩 阳 著
128 泛函微分方程的相空间理论及应用 2009.4 王 克 范 猛 著
129 概率论基础(第二版) 2009.8 严士健 王隽骧 刘秀芳 著
130 自相似集的结构 2010.1 周作领 瞿成勤 朱智伟 著
131 现代统计研究基础 2010.3 王启华 史宁中 耿 直 主编

132　图的可嵌入性理论(第二版)　2010.3　刘彦佩　著
133　非线性波动方程的现代方法(第二版)　2010.4　苗长兴　著
134　算子代数与非交换 L_p 空间引论　2010.5　许全华　吐尔德别克　陈泽乾　著
135　非线性椭圆型方程　2010.7　王明新　著
136　流形拓扑学　2010.8　马　天　著
137　局部域上的调和分析与分形分析及其应用　2011.6　苏维宜　著
138　Zakharov 方程及其孤立波解　2011.6　郭柏灵　甘在会　张景军　著
139　反应扩散方程引论(第二版)　2011.9　叶其孝　李正元　王明新　吴雅萍　著
140　代数模型论引论　2011.10　史念东　著
141　拓扑动力系统——从拓扑方法到遍历理论方法　2011.12　周作领　尹建东　许绍元　著
142　Littlewood-Paley 理论及其在流体动力学方程中的应用　2012.3　苗长兴　吴家宏　章志飞　著
143　有约束条件的统计推断及其应用　2012.3　王金德　著
144　混沌、Mel′nikov 方法及新发展　2012.6　李继彬　陈凤娟　著
145　现代统计模型　2012.6　薛留根　著
146　金融数学引论　2012.7　严加安　著
147　零过多数据的统计分析及其应用　2013.1　解锋昌　韦博成　林金官　编著
148　分形分析引论　2013.6　胡家信　著
149　索伯列夫空间导论　2013.8　陈国旺　编著
150　广义估计方程估计方法　2013.8　周　勇　著
151　统计质量控制图理论与方法　2013.8　王兆军　邹长亮　李忠华　著
152　有限群初步　2014.1　徐明曜　著
153　拓扑群引论(第二版)　2014.3　黎景辉　冯绪宁　著
154　现代非参数统计　2015.1　薛留根　著
155　三角范畴与导出范畴　2015.5　章　璞　著
156　线性算子的谱分析(第二版)　2015.6　孙　炯　王　忠　王万义　编著
157　双周期弹性断裂理论　2015.6　李　星　路见可　著
158　电磁流体动力学方程与奇异摄动理论　2015.8　王　术　冯跃红　著
159　算法数论(第二版)　2015.9　裴定一　祝跃飞　编著
160　偏微分方程现代理论引论　2016.1　崔尚斌　著
161　有限集上的映射与动态过程——矩阵半张量积方法　2015.11　程代展　齐洪胜　贺风华　著
162　现代测量误差模型　2016.3　李高荣　张　君　冯三营　著
163　偏微分方程引论　2016.3　韩丕功　刘朝霞　著
164　半导体偏微分方程引论　2016.4　张凯军　胡海丰　著
165　散乱数据拟合的模型、方法和理论(第二版)　2016.6　吴宗敏　著

166　交换代数与同调代数(第二版)　2016.12　李克正　著
167　Lipschitz 边界上的奇异积分与 Fourier 理论　2017.3　钱　涛　李澎涛　著
168　有限 p 群构造(上册)　2017.5　张勤海　安立坚　著
169　有限 p 群构造(下册)　2017.5　张勤海　安立坚　著